McAfee®

Wireless Protection 2007

Benutzerhandbuch

Inhalt

McAfee Wireless Protection 5

McAfee SecurityCenter 7

Funktionen ... 8
Verwenden von SecurityCenter ... 9
Header ... 9
Linke Spalte ... 9
Hauptbereich ... 10
Erläuterungen zu den SecurityCenter-Symbolen ... 11
Erläuterungen zum Schutzstatus ... 13
Beheben von Sicherheitsproblemen ... 19
Anzeigen der SecurityCenter-Informationen ... 20
Verwenden des Menüs "Erweitert" ... 21
Konfigurieren von SecurityCenter-Optionen ... 23
Konfigurieren des Schutzstatus ... 24
Konfigurieren von Benutzeroptionen ... 25
Konfigurieren der Update-Optionen ... 29
Konfigurieren von Alarmoptionen ... 35
Ausführen häufiger Tasks ... 37
Ausführen häufiger Tasks ... 37
Zuletzt aufgetretene Ereignisse anzeigen ... 38
Automatisches Warten Ihres Computers ... 39
Manuelles Warten Ihres Computers ... 40
Verwalten Ihres Netzwerks ... 42
Weitere Informationen zu Viren ... 42

McAfee QuickClean 43

Erläuterungen zu den QuickClean-Funktionen ... 44
Funktionen ... 44
Bereinigen Ihres Computers ... 45
Verwenden von QuickClean ... 47

McAfee Shredder 49

Erläuterungen zu den Funktionen von Shredder ... 50
Funktionen ... 50
Vernichten unerwünschter Dateien mit Shredder ... 51
Verwenden von Shredder ... 52

McAfee Network Manager 55

Funktionen ... 56
Erläuterung der Network Manager-Symbole ... 57
Erstellen eines verwalteten Netzwerks ... 59
Arbeiten mit der Netzwerkzuordnung ... 60
Anmelden am verwalteten Netzwerk ... 63
Remote-Verwaltung des Netzwerks ... 69
Überwachen des Status und der Berechtigungen ... 70
Beheben von Sicherheitslücken ... 73

McAfee Wireless Network Security 75

Funktionen ... 76
Wireless Network Security starten ... 78
Wireless Network Security starten ... 78
Wireless Network Security deaktivieren ... 79
Drahtlose Netzwerke schützen ... 81
Geschützte drahtlose Netzwerke einrichten ... 82
Computer zum geschützten drahtlosen Netzwerk hinzufügen ... 95
Drahtlosen Netzwerken verwalten ... 99
Verwalten drahtloser Netzwerke ... 100
Sicherheit für drahtloses Netzwerk verwalten ... 113
Konfigurieren von Sicherheitseinstellungen ... 114
Netzwerkschlüssel verwalten ... 119
Drahtlose Netzwerke überwachen ... 129
Drahtlose Netzwerkverbindungen überwachen ... 130
Geschützte drahtlose Netzwerke überwachen ... 136
Problembehandlung ... 141

McAfee EasyNetwork 159

Funktionen ... 160
EasyNetwork einrichten ... 161
Starten von EasyNetwork ... 162
Anmelden an einem verwalteten Netzwerk ... 163
Verwaltetes Netzwerk verlassen ... 167
Dateien freigeben und senden ... 169
Dateien freigeben ... 170
Senden von Dateien an andere Computer ... 173
Drucker freigeben ... 175
Mit freigegebenen Druckern arbeiten ... 176

Referenz 179

Glossar 180

Info zu McAfee 199

Copyright 200

Index 201

KAPITEL 1

McAfee Wireless Protection

McAfee Wireless Protection Suite behebt Netzwerkprobleme und eliminiert Risiken drahtloser Netzwerke. Der zuverlässige Schutz verhindert, dass Hacker Ihr Wi-Fi(R)-Netzwerk angreifen, schützt Ihre persönlichen Informationen und Transaktionen und hält andere davon ab, über Ihr Netzwerk auf das Internet zuzugreifen - und das mit einem einzigen Mausklick. Die leistungsstarken, rotierenden Verschlüsselungsschlüssel von McAfee Wireless Network Security halten selbst den hartnäckigsten Eindringling von Ihrem drahtlosen Netzwerk fern. Wireless Protection beinhaltet außerdem McAfee EasyNetwork, mit dem Sie problemlos Dateien und Drucker in Ihrem Netzwerk freigeben können. Zusätzlich enthält es McAfee Network Manager, der Computer in Ihrem Netzwerk auf Sicherheitslücken überwacht und potentielle Sicherheitsprobleme problemlos behebt.

Wireless Protection enthält folgende Programme:

- SecurityCenter
- Wireless Network Security
- Network Manager
- EasyNetwork

KAPITEL 2

McAfee SecurityCenter

McAfee SecurityCenter ist eine benutzerfreundliche Umgebung, in der McAfee-Benutzer ihre Sicherheitsabonnements starten, verwalten und konfigurieren können.

SecurityCenter dient außerdem als Informationsquelle für Viruswarnungen, Produktinformationen, Support und Abonnementinformationen sowie als schnelle Verbindung zu den Tools und News auf der McAfee-Website.

In diesem Kapitel

Funktionen 8
Verwenden von SecurityCenter 9
Konfigurieren von SecurityCenter-Optionen 23
Ausführen häufiger Tasks 37

Funktionen

McAfee SecurityCenter bietet folgende neue Funktionen und Vorteile:

Neu entworfener Sicherheitsstatus

Vereinfacht es, den Sicherheitsstatus Ihres Computers zu prüfen, nach Updates zu suchen und potentielle Sicherheitsrisiken zu beseitigen.

Ständige Updates und Upgrades

Installiert automatisch tägliche Updates. Wenn eine neue Version von McAfee verfügbar wird, erhalten Sie diese während der Laufzeit Ihres Abonnements automatisch, so dass gewährleistet wird, dass Sie stets über den aktuellsten Schutz verfügen.

Warnungen in Echtzeit

Sicherheitswarnungen benachrichtigen Sie über den Ausbruch neuer Viren und Sicherheitsbedrohungen. Sie bieten auch Reaktionsoptionen zum Entfernen und Neutralisieren der Bedrohung und enthalten weitere Informationen dazu.

Umfassender Schutz

Eine Vielzahl von Erneuerungsoptionen, so dass Ihr McAfee-Schutz stets auf dem aktuellsten Stand ist.

Leistungs-Tools

Entfernt nicht verwendete Dateien, defragmentiert verwendete Dateien und verwendet die Systemwiederherstellung, um Ihren Computer auf höchstem Leistungsniveau zu halten.

Echte Online-Hilfe

Unterstützung von Experten für Computer-Sicherheit von McAfee über den Internet-Chat, per E-Mail oder das Telefon.

Schutz für sicheres Surfen

Das McAfee SiteAdvisor-Browser-Plugin hilft Ihnen, sofern installiert, sich vor Spyware, Spam, Viren und Online-Bedrohungen zu schützen, indem es Websites klassifiziert, die Sie besuchen, oder die in Ihren Web-Suchergebnissen angezeigt werden. Sie erhalten ausführliche Sicherheitsklassifizierungen, die belegen, wie eine Site beim Test der E-Mail-Praktiken, Downloads, Online-Zugehörigkeiten und Störungen, z. B. Popups und Nachverfolgungs-Cookies von Fremdherstellern, abgeschnitten hat.

KAPITEL 3

Verwenden von SecurityCenter

SecurityCenter wird über das McAfee SecurityCenter-Symbol im Windows-Benachrichtigungsbereich rechts neben der Taskleiste oder über Ihren Windows-Desktop gestartet.

Wenn Sie SecurityCenter öffnen, wird im Bereich "Home" der Schutzstatus Ihres Computers angezeigt, und Sie erhalten schnellen Zugriff auf Update-, Scan (falls McAfee VirusScan installiert ist) und andere häufig auftretende Tasks:

Header

Hilfe

Anzeigen der Hilfedatei zur Anwendung

Linke Spalte

Aktualisieren

Aktualisieren Sie Ihr Produkt, um zu gewährleisten, dass Ihr Computer vor den neuesten Bedrohungen geschützt ist.

Scannen

Falls McAfee VirusScan installiert ist, können Sie einen manuellen Scan Ihres Computers durchführen.

Häufige Tasks

Führen Sie häufig vorkommende Tasks aus, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Verwaltens Ihres Computer-Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Wartens Ihres Computers. Falls McAfee Data Backup installiert ist, können Sie auch Ihre Daten sichern.

Komponenten installiert

Hier sehen Sie, welche Sicherheitsdienste die Sicherheit Ihres Computers schützen.

Hauptbereich

Sicherheitsstatus

Unter **Bin ich geschützt** finden Sie die allgemeine Ebene für den Schutzstatus Ihres Computers. Darunter können Sie Details zu diesem Status nach der Schutzkategorie und dem Schutztyp anzeigen.

SecurityCenter-Informationen

Zeigen Sie an, wann die letzte Aktualisierung Ihres Computers stattgefunden hat, wann der letzte Scan durchgeführt wurde (falls McAfee VirusScan installiert ist) und wann Ihr Abonnement abläuft.

In diesem Kapitel

Erläuterungen zu den SecurityCenter-Symbolen.....11
Erläuterungen zum Schutzstatus.....13
Beheben von Sicherheitsproblemen 19
Anzeigen der SecurityCenter-Informationen 20
Verwenden des Menüs "Erweitert".....21

Erläuterungen zu den SecurityCenter-Symbolen

In Ihrem Windows-Benachrichtigungsbereich werden SecurityCenter-Symbole rechts neben der Taskleiste angezeigt. Verwenden Sie diese Symbole, um zu erkennen, ob Ihr Computer umfassend geschützt ist, ob gerade ein Scan durchgeführt wird (falls McAfee VirusScan installiert ist), ob Updates vorliegen, um kürzlich aufgetretene Ereignisse anzuzeigen, Ihren Computer zu warten und Support von der McAfee-Website zu erhalten.

Öffnen von SecurityCenter und Verwenden der zusätzlichen Funktionen

Wenn SecurityCenter ausgeführt wird, wird das SecurityCenter M-Symbol rechts neben der Taskleiste im Windows-Systembereich angezeigt.

So öffnen Sie SecurityCenter und verwenden die zusätzlichen Funktionen:

- Klicken Sie mit der rechten Maustaste auf das Hauptsymbol von SecurityCenter, und klicken Sie anschließend auf eine der folgenden Optionen:
  - SecurityCenter öffnen
  - Updates
  - Direkte Links

    Das Untermenü enthält Links zu "Home", "Kürzlich aufgetretene Ereignisse", "Netzwerk verwalten", "Computer warten" und "Datensicherung" (falls installiert).
  - Abonnement überprüfen

    (Dieses Element wird angezeigt, wenn mindestens ein Produkt-Abonnement abgelaufen ist.)
  - Upgrade Center
  - Kundendienst

Prüfen Ihres Schutzstatus

Wenn Ihr Computer nicht umfassend geschützt ist, wird das Symbol für den Schutzstatus rechts neben der Taskleiste im Windows-Systembereich angezeigt. Das Symbol kann je nach dem Schutzstatus rot oder gelb sein.

So prüfen Sie Ihren Schutzstatus:

- Klicken Sie auf das Symbol für den Schutzstatus, um SecurityCenter zu öffnen und etwaige Probleme zu beheben.

Prüfen des Status Ihrer Updates

Wenn Sie auf Updates prüfen, wird das Updates-Symbol rechts neben der Taskleiste im Windows-Systembereich angezeigt.

So prüfen Sie den Status Ihrer Updates:

- Zeigen Sie auf das Updates-Symbol, um den Status Ihrer Updates als Quickinfo anzuzeigen.

Erläuterungen zum Schutzstatus

Der Gesamtschutzstatus Ihres Computers wird im Abschnitt **Bin ich geschützt?** von SecurityCenter dargestellt.

Der Schutzstatus informiert Sie darüber, ob Ihr Computer umfassend gegen die neuesten Sicherheitsbedrohungen geschützt ist oder ob Probleme Ihre Aufmerksamkeit verlangen. Sie finden hier außerdem Informationen zur Behebung dieser Probleme. Wenn ein Problem mehr als eine Schutzkategorie betrifft, kann das Beheben dieses Problems dazu führen, dass mehrere Kategorien wieder den Status für umfassenden Schutz erreichen.

Zu den Faktoren für den Schutzstatus zählen externe Sicherheitsbedrohungen, die auf dem Computer installierten Sicherheitsprodukte, Produkte mit Zugriff auf das Internet sowie deren Konfiguration.

Standardmäßig werden diese nicht kritischen Sicherheitsprobleme ignoriert und nicht im Gesamtschutzstatus protokolliert, wenn Spam-Schutz oder Inhaltsblockierung nicht installiert sind. Wenn ein Sicherheitsproblem jedoch von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten.

Bin ich geschützt?

Informationen zur Gesamtebene des Schutzstatus Ihres Computers finden Sie unter **Bin ich geschützt** in SecurityCenter.

- **Ja** wird angezeigt, wenn Ihr Computer umfassend geschützt ist (grün).
- **Nein** wird angezeigt, wenn Ihr Computer teilweise geschützt (gelb) oder nicht geschützt (rot) ist.

Um die meisten Sicherheitsprobleme automatisch zu lösen, klicken Sie neben dem Schutzstatus auf **Beheben**. Wenn jedoch ein oder mehrere Probleme weiterhin bestehen und Ihre Reaktion erfordern, klicken Sie auf den Link nach dem Problem, um die empfohlene Aktion auszuführen.

Erläuterungen zu den Schutzkategorien und -typen

Unter **Bin ich geschützt** in SecurityCenter können Sie Details zum Status anzeigen, aufgeschlüsselt nach den folgenden Schutzkategorien und -typen:

- Computer und Dateien
- Internet und Netzwerk
- E-Mail und IM
- Parental Controls

Die in SecurityCenter angezeigten Schutztypen hängen davon ab, welche Produkte installiert sind. Wenn beispielsweise der PC Health-Schutztyp angezeigt wird, ist die McAfee-Datensicherungssoftware installiert.

Wenn in einer Kategorie keine Sicherheitsprobleme vorliegen, ist der Status "grün". Wenn Sie auf eine grüne Kategorie klicken, wird rechts eine Liste der aktivierten Schutztypen angezeigt, gefolgt von einer Liste der bereits ignorierten Probleme. Wenn keine Probleme vorliegen, wird eine Virushinweis statt der Probleme angezeigt. Sie können auch auf **Konfigurieren** klicken, um Ihre Optionen für diese Kategorie zu ändern.

Wenn alle Schutztypen in einer Kategorie den Status "grün" aufweisen, ist der Status der Kategorie insgesamt "grün". Wenn alle Schutzkategorien den Status "grün" aufweisen, ist der Schutzstatus insgesamt "grün".

Wenn eine der Schutzkategorien den Status "gelb" oder "rot" aufweist, können Sie die Sicherheitsprobleme lösen, indem Sie sie beheben oder ignorieren, wodurch sich der Status in "grün" ändert.

Erläuterungen zum Schutz von Computer und Dateien

Die Schutzkategorie "Computer und Dateien" umfasst die folgenden Schutztypen:

- **Virenschutz**: Der Echtzeit-Scan-Schutz schützt Ihren Computer vor Viren, Würmern, Trojanern, verdächtigen Skripts, Hybridangriffen und anderen Bedrohungen. Das Programm führt automatische Scans durch und versucht, die Dateien zu säubern (einschließlich komprimierter .exe-Dateien, des Boot-Sektors, des Speichers und wichtiger Dateien), wenn Sie oder Ihr Computer darauf zugreifen.
- **Spyware-Schutz**: Der Spyware-Schutz dient zur raschen Erkennung, Blockierung und Entfernung von Spyware, Adware und anderen potentiell unerwünschten Programmen, die Ihre persönlichen Daten sammeln und ohne Ihre Zustimmung weiterleiten.
- **SystemGuards**: SystemGuards erkennt Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus. Sie können diese Änderungen prüfen und entscheiden, ob Sie sie erlauben möchten.
- **Windows-Schutz**: Der Windows-Schutz gibt den Status des Windows-Updates auf Ihrem Computer an. Wenn McAfee VirusScan installiert ist, steht außerdem der Pufferüberlaufschutz zur Verfügung.

Einer der Faktoren für den Schutz von Computer und Dateien sind externe Virusbedrohungen. Schützt beispielsweise Ihre Antivirensoftware Ihren Computer, wenn ein Virenausbruch stattfindet? Zu den weiteren Faktoren gehören die Konfiguration Ihrer Antivirensoftware und ob Ihre Software fortlaufend mit den neuesten Erkennungssignaturdateien aktualisiert wird, damit der Schutz Ihres Computers vor den neuesten Bedrohungen gewährleistet bleibt.

Öffnen des Konfigurationsbereichs für "Computer und Dateien"

Wenn unter **Computer & Dateien** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Computer und Dateien":

1. Klicken Sie im Home-Bereich auf **Computer & Dateien**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zum Schutz von Internet und Netzwerk

Die Schutzkategorie "Internet und Netzwerk" umfasst die folgenden Schutztypen:

- **Firewall-Schutz**: Der Firewall-Schutz schützt Ihren Computer vor Intrusionen und unerwünschtem Netzwerkverkehr. Gewährt alle eingehenden und ausgehenden Internetverbindungen.
- **Drahtloser Schutz**: Der drahtlose Schutz schützt Ihr privates drahtloses Netzwerk vor Intrusionen und Datenabfang. Wenn Sie jedoch derzeit mit einem externen drahtlosen Netzwerk verbunden sind, variiert Ihr Schutz in Abhängigkeit der Sicherheitsebene dieses Netzwerks.
- **Web-Browsing-Schutz**: Der Web-Browsing-Schutz verhindert, dass auf Ihrem Computer Werbung, Popups und Web-Bugs ausgeführt werden, während Sie im Internet surfen.
- **Phishing-Schutz**: Der Phishing-Schutz hilft dabei, betrügerische Websites zu blockieren, die über Hyperlinks in E-Mails und Instant Messages, Popups und anderen Quellen persönliche Informationen abrufen.
- **Personal Information Protection**: Personal Information Protection blockiert die Veröffentlichung wichtiger und vertraulicher Daten im Internet.

Öffnen des Konfigurationsbereichs für "Internet und Netzwerk"

Wenn unter **Internet & Netzwerk** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Internet und Netzwerk":

1. Klicken Sie im Home-Bereich auf **Internet & Netzwerk**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zu E-Mail- und IM-Schutz

Die Schutzkategorie "E-Mail- und IM-Schutz" umfasst die folgenden Schutztypen:

- **E-Mail-Schutz**: Der E-Mail-Schutz führt automatische Scans durch und versucht, Viren, Spyware und potentielle Bedrohungen in eingehenden und ausgehenden E-Mail-Nachrichten und -Anhängen zu säubern.
- **Spam-Schutz**: Der Spam-Schutz hilft Ihnen, Ihren E-Mail-Posteingang frei von unerwünschten E-Mails zu halten.
- **IM-Schutz**: Der Instant Messaging (IM)-Schutz führt automatische Scans durch und versucht, Viren, Spyware und potentielle Bedrohungen in eingehenden Instant Messaging-Nachrichten zu säubern. Das Programm verhindert außerdem, dass Instant Messaging-Clients unerwünschte Inhalte oder persönliche Informationen über das Internet austauschen.
- **Schutz für sicheres Surfen**: Falls installiert, hilft das McAfee SiteAdvisor-Browser-Plugin dabei, Ihren Computer vor Spyware, Spam, Viren und Online-Scams zu schützen, indem es Websites bewertet, die Sie besuchen oder die in Ihren Web-Suchergebnissen angezeigt werden. Sie können detaillierte Sicherheitsbewertungen anzeigen, aus denen hervorgeht, wie eine Site auf E-Mail-Praktiken, Downloads, Online-Partnerschaften und störende Praktiken, wie Popups und Verfolgungs-Cookies von Drittanbietern, getestet wird.

Öffnen des Konfigurationsbereichs für "E-Mail und IM"

Wenn unter **E-Mail & IM** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "E-Mail und IM"

1. Klicken Sie im Home-Bereich auf **E-Mail & IM**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zum Parental Controls-Schutz

Die Schutzkategorie "Parental Controls" umfasst die folgenden Schutztypen:

- **Parental Controls**: Die Inhaltsblockierung verhindert, dass Benutzer unerwünschte Internet-Inhalte anzeigen, indem potentiell schädliche Websites blockiert werden. Die Internetaktivitäten und die -nutzung der Benutzer können außerdem überwacht und eingeschränkt werden.

Öffnen des Konfigurationsbereichs für "Parental Controls"

Wenn unter **Parental Controls** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Parental Controls":

1. Klicken Sie im Home-Bereich auf **Parental Controls**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Beheben von Sicherheitsproblemen

Die meisten Sicherheitsprobleme können automatisch behoben werden. Wenn ein oder mehrere Probleme dennoch weiterhin vorliegen, müssen Sie sie lösen.

Automatisches Beheben von Sicherheitsproblemen

Die meisten Sicherheitsprobleme können automatisch behoben werden.

So beheben Sie Sicherheitsprobleme automatisch:

- Klicken Sie neben dem Schutzstatus auf **Beheben**.

Manuelles Beheben von Sicherheitsproblemen

Wenn ein oder mehrere Probleme nicht automatisch behoben werden, klicken Sie auf den Link nach dem Problem, um die empfohlene Aktion auszuführen.

So beheben Sie Sicherheitsprobleme manuell:

- Führen Sie einen der folgenden Vorgänge aus:
  - Wenn innerhalb der letzten 30 Tage kein vollständiger Scan Ihres Computers durchgeführt wurde, klicken Sie links neben dem HauptSchutzstatus auf **Scannen**, um einen manuellen Scan durchzuführen. (Dieses Element wird angezeigt, wenn McAfee VirusScan installiert ist.)
  - Wenn Ihre Virusdefinitionsdateien (DAT) veraltet sind, klicken Sie links neben dem HauptSchutzstatus auf **Update**, um Ihren Schutz zu aktualisieren.
  - Wennn ein Programm nicht installiert ist, klicken Sie für die Installation auf **Erhalten Sie vollständigen Schutz**.
  - Wenn Komponenten für ein Programm fehlen, installieren Sie es erneut.
  - Wenn ein Programm registriert sein muss, um vollständigen Schutz zu erhalten, klicken Sie zur Registrierung auf **Jetzt registrieren**. (Dieses Element wird angezeigt, wenn ein oder mehrere Programme abgelaufen sind.)
  - Wenn ein Programm abgelaufen ist, klicken Sie auf **Mein Abonnement jetz überprüfen**, um Ihren Kontostatus zu prüfen. (Dieses Element wird angezeigt, wenn ein oder mehrere Programme abgelaufen sind.)

Anzeigen der SecurityCenter-Informationen

Im unteren Teil des Schutzstatusbereichs bieten Ihnen die SecurityCenter-Informationen Zugriff auf SecurityCenter-Optionen. Sie sehen hier außerdem, wann das letzte Update sowie der letzte Scan durchgeführt wurden (falls McAfee VirusScan installiert ist) und wann die Abonnements für Ihre McAfee-Produkte ablaufen.

Öffnen des SecurityCenter-Konfigurationsbereichs

Sie können den SecurityCenter-Konfigurationsbereich öffnen, um Ihre Optionen im Home-Bereich zu ändern.

So öffnen Sie den SecurityCenter-Konfigurationsbereich:

- Klicken Sie im Home-Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.

Anzeigen von Informationen zum installierten Produkt

Sie können eine Liste der installierten Produkte anzeigen, in der Sie die Versionsnummer des Produkts und den Zeitpunkt der letzten Aktualisierung sehen.

So zeigen Sie Ihre McAfee-Produktinformationen an:

- Klicken Sie im Home-Bereich unter **SecurityCenter-Informationen** auf die Option **Details anzeigen**, um das Fenster mit Produktinformationen zu öffnen.

Verwenden des Menüs "Erweitert"

Wenn Sie SecurityCenter zum ersten Mal öffnen, wird in der linken Spalte das Menü "Grundlagen" angezeigt. Wenn Sie ein erfahrener Benutzer sind, können Sie auf das Menü **Erweitert** klicken, um ein detaillierteres Menü mit Befehlen an dieser Stelle anzuzeigen. Das zuletzt verwendete Menü wird angezeigt, wenn Sie SecurityCenter das nächste Mal verwenden.

Das Menü "Erweitert" umfasst die folgenden Elemente:

- Home
- Berichte und Protokolle (umfasst die Liste "Zuletzt aufgetretene Ereignisse" und Protokolle für die letzten 30, 60 und 90 Tage nach dem Typ geordnet)
- Konfigurieren
- Wiederherstellen
- Extras

KAPITEL 4

Konfigurieren von SecurityCenter-Optionen

SecurityCenter zeigt den Schutzstatus Ihres Computers insgesamt, ermöglicht Ihnen das Erstellen von McAfee-Benutzerkonten, installiert automatisch die neuesten Produkt-Updates und benachrichtigt Sie automatisch mit Warnmeldungen und -signalen bei öffentlichen Virenausbrüchen, Sicherheitsbedrohungen und Produkt-Updates.

Im SecurityCenter-Konfigurationsbereich können Sie Ihre SecurityCenter-Optionen für die folgenden Funktionen ändern:

- Schutzstatus
- Benutzer
- Automatische Updates
- Warnungen

In diesem Kapitel

Konfigurieren des Schutzstatus.....24
Konfigurieren von Benutzeroptionen.....25
Konfigurieren der Update-Optionen.....29
Konfigurieren von Alarmoptionen.....35

Konfigurieren des Schutzstatus

Der Gesamtschutzstatus Ihres Computers wird im Abschnitt **Bin ich geschützt?** von SecurityCenter dargestellt.

Der Schutzstatus informiert Sie darüber, ob Ihr Computer umfassend gegen die neuesten Sicherheitsbedrohungen geschützt ist oder ob Probleme Ihre Aufmerksamkeit verlangen. Sie finden hier außerdem Informationen zur Behebung dieser Probleme.

Standardmäßig werden diese nicht kritischen Sicherheitsprobleme ignoriert und nicht im Gesamtschutzstatus protokolliert, wenn Spam-Schutz oder Inhaltsblockierung nicht installiert sind. Wenn ein Sicherheitsproblem jedoch von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten. Wenn Sie zu einem späteren Zeitpunkt beschließen, dass Sie ein zuvor ignoriertes Problem beheben möchten, können Sie das Problem zur Nachverfolgung in den Schutzstatus aufnehmen.

Konfigurieren ignorierter Probleme

Sie können Probleme als Teil des Schutzstatus Ihres Computers insgesamt in die Nachverfolgung aufnehmen oder davon ausschließen. Wenn ein Sicherheitsproblem von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten. Wenn Sie zu einem späteren Zeitpunkt beschließen, dass Sie ein zuvor ignoriertes Problem beheben möchten, können Sie das Problem zur Nachverfolgung in den Schutzstatus aufnehmen.

So konfigurieren Sie ignorierte Probleme:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Schutzstatus**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Führen Sie im Bereich "Ignorierte Probleme" einen der folgenden Schritte aus:
   - Um zuvor ignorierte Probleme in den Schutzstatus mit aufzunehmen, aktivieren Sie die entsprechenden Kontrollkästchen.
   - Um Probleme aus dem Schutzstatus auszuschließen, wählen Sie die entsprechenden Kontrollkästchen aus.
4. Klicken Sie auf **OK**.

Konfigurieren von Benutzeroptionen

Wenn Sie Programme von McAfee ausführen, für die Benutzerberechtigungen erforderlich sind, entsprechen diese Berechtigungen standardmäßig den Windows-Benutzerkonten auf diesem Computer. Um die Benutzerverwaltung für diese Programme einfacher zu gestalten, können Sie jederzeit dazu übergehen, McAfee-Benutzerkonten zu verwenden.

Wenn Sie zur Verwendung von McAfee-Benutzerkonten übergehen, werden bestehende Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm automatisch importiert. Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, müssen Sie jedoch ein Administratorkonto erstellen. Danach können Sie mit der Erstellung und Konfigurierung anderer McAfee-Benutzerkonten beginnen.

Übergehen zur Verwendung von McAfee-Benutzerkonten

Standardmäßig werden Windows-Benutzerkonten verwendet. Beim Wechseln zu McAfee-Benutzerkonten ist das Erstellen von zusätzlichen Windows-Benutzerkonten jedoch nicht mehr erforderlich.

So gehen Sie zur Verwendung von McAfee-Benutzerkonten über:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Benutzer**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Um McAfee-Benutzerkonten zu verwenden, klicken Sie auf **Wechseln**.

Wenn Sie zum ersten Mal McAfee-Benutzerkonten verwenden, müssen Sie ein Administratorkonto erstellen (Seite 26).

Erstellen eines Administratorkontos

Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, werden Sie aufgefordert, ein Administratorkonto zu erstellen.

So erstellen Sie ein Administratorkonto:

1. Geben Sie im Feld **Kennwort** ein Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
2. Wählen Sie aus der Liste eine Frage zur Wiederbeschaffung des Kennworts aus, und geben Sie die Antwort auf die geheime Frage in das Kästchen **Antwort** ein.
3. Klicken Sie auf **Übernehmen**.

   Wenn Sie fertig sind, wird der Benutzerkontotyp im entsprechenden Feld mit den bestehenden Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm aktualisiert, falls zutreffend. Wenn Sie zum ersten Mal Benutzerkonten konfigurieren, wird der Bereich "Benutzer verwalten" angezeigt.

Konfigurieren von Benutzeroptionen

Wenn Sie zur Verwendung von McAfee-Benutzerkonten übergehen, werden bestehende Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm automatisch importiert. Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, müssen Sie jedoch ein Administratorkonto erstellen. Danach können Sie mit der Erstellung und Konfiguration anderer McAfee-Benutzerkonten beginnen.

So konfigurieren Sie Benutzeroptionen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Benutzer**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Klicken Sie unter **Benutzerkonten** auf **Hinzufügen**.
4. Geben Sie in das Feld **Benutzername** einen Benutzernamen ein.
5. Geben Sie im Feld **Kennwort** ein Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
6. Wählen Sie das Kontrollkästchen **Startbenutzer** aus, wenn Sie diesen neuen Benutzer als Startbenutzer festlegen möchten, wenn SecurityCenter gestartet wird.
7. Wählen Sie unter **Benutzerkontotyp** einen Kontotyp für diesen Benutzer aus, und klicken Sie anschließend auf **Erstellen**.

   Hinweis: Nach dem Erstellen des Benutzerkontos müssen Sie unter "Parental Controls" die Einstellungen für einen Benutzer mit eingeschränkten Rechten konfigurieren.

8. Um das Kennwort eines Benutzers, die automatische Anmeldung oder den Kontotyp zu ändern, wählen Sie einen Benutzernamen aus der Liste aus, und klicken Sie auf **Bearbeiten**.
9. Klicken Sie auf **Übernehmen**.

Abrufen des Administratorkennworts

Wenn Sie das Administratorkennwort vergessen, können Sie es abrufen.

So rufen Sie das Administratorkennwort ab:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter M-Symbol, und klicken Sie anschließend auf **Benutzer wechseln**.
2. Wählen Sie in der Liste **Benutzername** die Option **Administrator** aus, und klicken Sie anschließend auf **Kennwort vergessen**.
3. Geben Sie die Antwort auf die von Ihnen bei der Erstellung des Administratorkontos angegebene geheime Frage ein.
4. Klicken Sie auf **Senden**.

   Ihr vergessenes Administratorkennwort wird angezeigt.

Ändern des Administratorkennworts

Wenn Sie sich nicht an Ihr Administratorkennwort erinnern oder vermuten, dass es missbraucht worden sein könnte, können Sie es ändern.

So ändern Sie das Administratorkennwort:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter M-Symbol, und klicken Sie anschließend auf **Benutzer wechseln**.
2. Wählen Sie in der Liste **Benutzername** die Option **Administrator** aus, und klicken Sie anschließend auf **Kennwort ändern**.
3. Geben Sie im Feld **Altes Kennwort** Ihr bestehendes Kennwort ein.
4. Geben Sie im Feld **Kennwort** das neue Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
5. Klicken Sie auf **OK**.

Konfigurieren der Update-Optionen

SecurityCenter prüft nach Herstellung einer Internetverbindung automatisch alle vier Stunden auf Updates für Ihre gesamten McAfee-Dienste. Die neuesten Produkt-Updates werden anschließend automatisch installiert. Sie können auch jederzeit manuell prüfen, ob Updates vorliegen, indem Sie rechts neben der Taskleiste im Benachrichtigungsbereich auf das SecurityCenter-Symbol klicken.

Automatisches Prüfen auf Updates

Das Bestehen einer Internetverbindung vorausgesetzt, sucht SecurityCenter Online automatisch alle vier Stunden nach neuen Updates. Sie können SecurityCenter auch so konfigurieren, dass Sie benachrichtigt werden, bevor Updates heruntergeladen oder installiert werden.

So prüfen Sie automatisch auf Updates:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Automatische Updates aktiviert**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Wählen Sie im Bereich "Update-Optionen" einen der folgenden Schritte aus:
   - Updates automatisch installieren und benachrichtigen, wenn das Produkt aktualisiert wurde (empfohlene Einstellung) (Seite 30)
   - Updates automatisch herunterladen und benachrichtigen, wenn das Installationsprogramm startbereit ist (Seite 31)
   - Vor dem Herunterladen von Updates benachrichtigen (Seite 32)
4. Klicken Sie auf **OK**.

Hinweis: Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und diese ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatischen Updates deaktivieren (Seite 32).

Automatisches Herunterladen und Installieren von Updates

Wenn Sie in den SecurityCenter-Update-Optionen die Option **Updates automatisch installieren und benachrichtigen, wenn meine Dienste aktualisiert werden (empfohlene Einstellung)** auswählen, werden Updates automatisch von SecurityCenter heruntergeladen und installiert.

Automatisches Herunterladen von Updates

Wenn Sie in den Update-Optionen die Option **Updates automatisch herunterladen und benachrichtigen, wenn das Installationsprogramm startbereit ist** auswählen, lädt SecurityCenter Updates automatisch herunter und benachrichtigt Sie, wenn ein Update installiert werden kann. Sie können dann entscheiden, ob Sie das Update installieren oder die Installation auf einen späteren Zeitpunkt verschieben möchten (Seite 33).

So installieren Sie ein automatisch heruntergeladenes Update:

1. Klicken Sie in der Warnung auf **Meine Produkte jetzt aktualisieren** und anschließend auf **OK**.

   Bei entsprechender Aufforderung müssen Sie sich auf der Website anmelden, damit Ihr Abonnement verifiziert werden kann. Der Download erfolgt erst nach der Verifizierung.

2. Nach der Verifizierung Ihres Abonnements klicken Sie im Bereich "Updates" auf **Update**, um das Update herunterzuladen und zu installieren. Wenn Ihr Abonnement abgelaufen ist, klicken Sie in dem diesbezüglichen Warnhinweis auf **Abonnement erneuern** und folgen dann den Eingabeaufforderungen.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Benachrichtigen vor dem Herunterladen von Updates

Wenn Sie im Bereich "Update-Optionen" **Benachrichtigen vor dem Herunterladen von Updates** aktiviert haben, werden Sie vor dem Herunterladen von Updates von SecurityCenter benachrichtigt. Sie können dann selbst entscheiden, ob Sie ein Update Ihrer Sicherheitsdienste herunterladen und installieren und damit die Gefahr eines Angriffs eliminieren möchten.

So laden und installieren Sie ein Update:

1. Klicken Sie in der Warnung auf **Meine Produkte jetzt aktualisieren** und anschließend auf **OK**.
2. Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden.

   Das Update wird automatisch heruntergeladen.
3. Klicken Sie nach Abschluss der Update-Installation in der Warnung auf **OK**.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Deaktivieren von automatischen Updates

Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatische Aktualisierung deaktivieren.

Hinweis: Prüfen Sie mindestens ein Mal wöchentlich, ob Updates verfügbar sind (Seite 34). Wenn Sie keine Updates installieren, sind die Sicherheitsmechanismen zum Schutz Ihres Computers nicht auf dem aktuellen Stand.

So deaktivieren Sie die automatische Aktualisierung:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Automatische Updates aktiviert**, um den Bereich zu erweitern.
3. Klicken Sie auf **Aus**.
4. Bestätigen Sie die Änderung, indem Sie auf **Ja** klicken.

   Der Status wird im Header aktualisiert.

Wenn Sie nach sieben Tagen nicht manuell prüfen, ob Updates zur Verfügung stehen, werden Sie durch eine Warnmeldung daran erinnert.

Verschieben von Updates auf einen späteren Zeitpunkt

Wenn Sie beim Empfang der Benachrichtigung zu beschäftigt sind, Ihre Sicherheitsdienste zu aktualisieren, können Sie wählen, ob Sie zu einem späteren Zeitpunkt daran erinnert werden möchten, oder die Nachricht ignorieren.

So verschieben Sie ein Update auf einen späteren Zeitpunkt:

- Führen Sie einen der folgenden Vorgänge aus:
  - Klicken Sie in der Warnung auf **Später erinnern** und anschließend auf **OK**.
  - Klicken Sie auf **Warnung schließen** und anschließend auf **OK**, um die Warnung zu schließen und keine Aktionen zu ergreifen.

Manuelles Prüfen auf Updates

SecurityCenter prüft nach Herstellung einer Internetverbindung automatisch alle vier Stunden auf Updates und installiert anschließend die neuesten Produkt-Updates. Sie können auch jederzeit manuell prüfen, ob Updates vorliegen, indem Sie rechts neben der Taskleiste im Windows-Benachrichtigungsbereich auf das SecurityCenter-Symbol klicken.

Hinweis: Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und diese ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatischen Updates deaktivieren (Seite 32).

So prüfen Sie manuell auf Updates:

1. Stellen Sie sicher, dass Ihr Computer mit dem Internet verbunden ist.
2. Klicken Sie in Ihrem Windows-Benachrichtigungsbereich rechts neben der Taskleiste mit der rechten Maustaste auf das SecurityCenter M-Symbol und klicken Sie anschließend auf **Aktualisierungen**.

   Während SecurityCenter nach Updates sucht, können Sie weiterhin andere Aufgaben damit durchführen.

   Es wird in Ihrem Windows-Benachrichtigungsbereich rechts neben der Taskleiste ein animiertes Symbol angezeigt. Wenn SecurityCenter den Vorgang abgeschlossen hat, wird das Symbol automatisch wieder ausgeblendet.
3. Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden, um Ihr Abonnement zu verifizieren.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Konfigurieren von Alarmoptionen

Sie werden standardmäßig von SecurityCenter durch Warnmeldungen und akustische Warnsignale benachrichtigt, wenn Virusausbrüche stattfinden, Sicherheitsrisiken vorliegen oder Produkt-Updates verfügbar sind. Sie können SecurityCenter jedoch auch so konfigurieren, dass nur Warnungen angezeigt werden, die Ihre unmittelbare Aufmerksamkeit erfordern.

Konfigurieren von Warnoptionen

Sie werden standardmäßig von SecurityCenter durch Warnmeldungen und akustische Warnsignale benachrichtigt, wenn Virusausbrüche stattfinden, Sicherheitsrisiken vorliegen oder Produkt-Updates verfügbar sind. Sie können SecurityCenter jedoch auch so konfigurieren, dass nur Warnungen angezeigt werden, die Ihre unmittelbare Aufmerksamkeit erfordern.

So konfigurieren Sie Warnoptionen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Warnungen**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Wählen Sie im Bereich "Warnoptionen" einen der folgenden Schritte aus:
   - **Bei einem öffentlichen Virusausbruch oder einer öffentlichen Sicherheitsbedrohung benachrichtigen**
   - **Informationswarnungen einblenden, wenn Gaming-Modus erkannt wird**
   - **Akustisches Signal bei Warnungen ausgeben**
   - **Splash-Bildschirm von McAfee beim Starten von Windows anzeigen**
4. Klicken Sie auf **OK**.

Hinweis: Damit zukünftig keine informativen Warnmeldungen von der Warnung selbst mehr anzeigt werden, klicken Sie auf **Diese Warnung nicht mehr anzeigen**. Sie können diese Warnmeldungen später im Bereich "Informationswarnungen" erneut aktivieren.

Konfigurieren von Informationswarnungen

Informationswarnungen benachrichtigen Sie bei Ereignissen, die Ihr unmittelbares Eingreifen nicht erforderlich machen. Wenn Sie informative Warnmeldungen von der Warnung selbst für die Zukunft deaktivieren, können Sie sie später im Bereich "Informationswarnungen" erneut aktivieren.

So konfigurieren Sie Informationswarnungen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Warnungen**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Klicken Sie unter **SecurityCenter-Konfiguration** auf die Option **Informationswarnungen**.
4. Deaktivieren Sie das Kontrollkästchen **Informationswarnungen verbergen**, und deaktivieren Sie anschließend die Kontrollkästchen für Warnungen, die Sie anzeigen möchten, in der Liste.
5. Klicken Sie auf **OK**.

KAPITEL 5

Ausführen häufiger Tasks

Sie können häufig vorkommende Tasks ausführen, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Verwaltens Ihres Computer-Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Wartens Ihres Computers. Falls McAfee Data Backup installiert ist, können Sie auch Ihre Daten sichern.

In diesem Kapitel

Ausführen häufiger Tasks 37
Zuletzt aufgetretene Ereignisse anzeigen.....38
Automatisches Warten Ihres Computers 39
Manuelles Warten Ihres Computers.....40
Verwalten Ihres Netzwerks.....42
Weitere Informationen zu Viren 42

Ausführen häufiger Tasks

Sie können häufig vorkommende Tasks ausführen, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Wartens Ihres Computers und des Verwaltens Ihres Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Sicherns Ihrer Daten (falls McAfee Datensicherung installiert ist).

So führen Sie häufig vorkommende Tasks aus:

- Führen Sie im Menü "Grundlagen" unter **Häufige Tasks** einen der folgenden Schritte aus:
  - Um zum Home-Bereich zurückzukehren, klicken Sie auf **Home**.
  - Um kürzlich aufgetretene, von Ihrer Sicherheitssoftware erkannte Ereignisse anzuzeigen, klicken Sie auf **Zuletzt aufgetretene Ereignisse**.
  - Um nicht verwendete Dateien zu entfernen, Ihre Daten zu defragmentieren und Ihren Computer auf die vorherigen Einstellungen zurückzusetzen, klicken Sie auf **Computer warten**.
  - Um Ihr Computer-Netzwerk zu verwalten, klicken Sie auf einem Computer mit Verwaltungskapazitäten für dieses Netzwerk auf **Netzwerk verwalten**.

Der Network Manager überwacht PCs in Ihrem gesamten Netzwerk auf Sicherheitsschwachstellen, damit Sie Sicherheitsprobleme im Netzwerk einfach identifizieren können.

- Um Sicherungskopien Ihrer Dateien zu erstellen, klicken Sie auf **Datensicherung**, wenn McAfee Datensicherung installiert ist.

  Automatische Sicherungen speichern Kopien Ihrer wichtigsten Dateien, wann immer Sie möchten, so dass Ihre Dateien auf einem CD-/DVD-, USB- oder einem externen oder Netzwerklaufwerk verschlüsselt und gespeichert werden.

Tipp: Sie können häufig vorkommende Tasks von zwei weiteren Orten aus durchführen (unter **Home** im Menü "Erweitert" und im Menü **QuickLinks** des SecurityCenter M-Symbols ganz rechts auf der Taskleiste). Sie können unter **Berichte und Protokolle** im Menü "Erweitert" auch kürzlich aufgetretene Ereignisse und umfassende Protokolle nach Typ geordnet anzeigen.

Zuletzt aufgetretene Ereignisse anzeigen

Kürzlich aufgetreten Ereignisse werden protokolliert, wenn Änderungen an Ihrem Computer vorgenommen werden. Die Beispiele umfassen das Aktivieren oder Deaktivieren eines Schutztyps, das Entfernen einer Bedrohung sowie das Blockieren eines Versuchs, eine Internetverbindung herzustellen. Sie können die 20 am häufigsten aufgetretenen Ereignisse sowie die Details dazu anzeigen.

Details zu diesen Ereignissen finden Sie in der Hilfedatei des jeweiligen Produkts.

So zeigen Sie die zuletzt aufgetretenen Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Aktuelle Ereignisse anzeigen**.

   Sämtliche kürzlich aufgetretenen Ereignisse werden in der Liste angezeigt, zusammen mit dem Datum und einer kurzen Beschreibung.

2. Wählen Sie unter **Zuletzt aufgetretene Ereignisse** ein Ereignis aus, um weitere Informationen im Detailbereich anzuzeigen.

   Unter **Ich möchte** werden alle verfügbaren Aktionen angezeigt.

3. Um eine umfassendere Liste mit Ereignissen anzuzeigen, klicken Sie auf **Protokoll anzeigen**.

Automatisches Warten Ihres Computers

Um wertvollen Speicherplatz auf Ihrer Festplatte frei zu machen und die Leistung Ihres Computers zu optimieren, können Sie QuickClean- oder Defragmentierungs-Task so planen, dass sie in regelmäßigen Zeitabständen ausgeführt werden. Diese Tasks umfassen das Löschen, Shreddern und Defragmentieren von Dateien und Ordnern.

So warten Sie Ihren Computer automatisch:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie auf **Taskplaner** auf **Start**.
3. Wählen Sie in der Vorgangsliste **QuickClean** oder **Defragmentierungsprogramm** aus.
4. Führen Sie einen der folgenden Vorgänge aus:
   - Um einen bestehenden Task zu verändern, wählen Sie den Task aus und klicken dann auf **Ändern**. Folgen Sie den Anweisungen auf dem Bildschirm.
   - Um einen neuen Task zu erstellen, geben Sie den Namen in das Feld **Taskname** ein und klicken anschließend auf **Erstellen**. Folgen Sie den Anweisungen auf dem Bildschirm.
   - Um einen Task zu löschen, wählen Sie ihn aus und klicken dann auf **Löschen**.
5. Zeigen Sie unter **Task-Zusammenfassung** an, wann der Task zuletzt ausgeführt wurde, wann er zum nächsten Mal ausgeführt wird sowie welchen Status er hat.

Manuelles Warten Ihres Computers

Sie können manuelle Wartungs-Tasks ausführen, um nicht verwendete Dateien zu entfernen, Ihre Daten zu defragmentieren und Ihren Computer auf die vorherigen Einstellungen zurückzusetzen.

So warten Sie Ihren Computer manuell:

- Führen Sie einen der folgenden Vorgänge aus:
  - Um QuickClean zu verwenden, klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, klicken Sie auf **Computer warten** und anschließend auf **Start**.
  - Um das Defragmentierungsprogramm zu verwenden, klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, klicken Sie auf **Computer warten**, und anschließend auf **Analysieren**.
  - Um die Systemwiederherstellung im Menü "Erweitert" zu verwenden, klicken Sie auf **Tools**, klicken Sie anschließend auf **Systemwiederherstellung** und dann auf **Start**.

Entfernen nicht verwendeter Dateien und Ordner

Verwenden Sie QuickClean, um wertvollen Speicherplatz frei zu machen und die Leistung Ihres Computers zu optimieren.

So entfernen Sie nicht verwendete Dateien und Ordner:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie unter **QuickClean** auf **Start**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Defragmentieren von Dateien und Ordnern

Die Dateifragmentierung findet statt, wenn Dateien und Ordner gelöscht und neue Dateien hinzugefügt werden. Durch die Fragmentierung wird der Festplattenzugriff verlangsamt und die Gesamtleistung Ihres Computers herabgesetzt, wenn normalerweise auch nicht sehr stark.

Verwenden Sie das Defragmentierungsprogramm, um Teile einer Datei auf aufeinanderfolgenden Sektoren auf einer Festplatte zu schreiben, um die Geschwindigkeit von Zugriff und Abruf zu erhöhen.

So defragmentieren Sie Dateien und Ordner:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie unter **Defragmentierungsprogramm** auf **Analysieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Zurücksetzen Ihres Computers auf die vorherigen Einstellungen

Wiederherstellungspunkte sind Kurzübersichten über Ihren Computer, die Windows in regelmäßigen Abständen speichert sowie wenn wichtige Ereignisse stattfinden (beispielsweise wenn ein Programm oder Treiber installiert wird). Sie können jdeoch auch jederzeit Ihre eigenen Wiederherstellungspunkte erstellen und diese benennen.

Verwenden Sie Wiederherstellungspunkte, um schädliche Änderungen an Ihrem Computer rückgängig zu machen und diesen auf die vorherigen Einstellungen zurückzusetzen.

So setzen Sie Ihren Computer auf die vorherigen Einstellungen zurück:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Systemwiederherstellung**.
2. Klicken Sie unter **Systemwiederherstellung** auf **Start**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Verwalten Ihres Netzwerks

Wenn Ihr Computer über Verwaltungskapazitäten für Ihr Netzwerk verfügt, können Sie Network Manager verwenden, um PCs in Ihrem gesamten Netzwerk auf Sicherheitsschwachstellen zu überwachen, damit Sie Sicherheitsprobleme einfach identifizieren können.

Wenn der Schutzstatus Ihres Computers in diesem Netzwerk nicht überwacht wird, ist Ihr Computer entweder nicht Teil dieses Netzwerks, oder es handelt sich um ein nicht verwaltetes Mitglied dieses Netzwerks. Weitere Details hierzu finden Sie in der Hilfedatei zu Network Manager.

So verwalten Sie Ihr Netzwerk:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Netzwerk verwalten**.
2. Klicken Sie auf das Symbol, das in der Netzwerkkarte für diesen Computer steht.
3. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.

Weitere Informationen zu Viren

Verwenden Sie die Vireninformationsbibliothek und die Virus Map, um folgende Aktionen durchzuführen:

- Erfahren Sie mehr zu den neuesten Viren, E-Mail-Virus-Hoaxes und anderen Bedrohungen.
- Erhalten Sie kostenlose Tools zur Virenentfernung, die Ihnen dabei helfen, Ihren Computer zu reparieren.
- Hier erfahren Sie aus der Vogelperspektive in Echtzeit, an welchen Orten der Welt derzeit PCs von Viren angegriffen werden.

So erhalten Sie weitere Informationen zu Viren:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Virusinformationen**.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Untersuchen von Viren mithilfe der McAfee-Virusinformationsbibliothek
   - Untersuchen von Viren mithilfe der World Virus Map auf der McAfee-Website

KAPITEL 6

McAfee QuickClean

Beim Surfen im Internet sammelt sich viel Müll auf Ihrem Computer an. Schützen Sie Ihre Privatsphäre und löschen Sie Müll aus dem Internet und E-Mails, die Sie nicht benötigen, mit QuickClean. QuickClean identifiziert und löscht Dateien, die sich beim Internetsurfen angesammelt haben, einschließlich unerwünschter Cookies, E-Mails, Downloads und des Verlaufs - Daten, die persönliche Informationen über Sie enthalten. Es schützt Ihre Privatsphäre durch das sichere Löschen dieser sensiblen Informationen.

QuickClean löscht außerdem unerwünschte Programme. Legen Sie fest, welche Dateien eliminiert werden sollen, und sorgen Sie für Ordnung, ohne dabei wesentliche Informationen zu löschen.

In diesem Kapitel

Erläuterungen zu den QuickClean-Funktionen 44
Bereinigen Ihres Computers 45

Erläuterungen zu den QuickClean-Funktionen

In diesem Abschnitt werden die Funktionen von QuickClean beschrieben.

Funktionen

QuickClean bietet einen Satz an effizienten und leicht zu verwendenden Tools, mit denen digitale Überschussdaten sicher gelöscht werden können. Sie können wertvollen Festplattenspeicherplatz frei geben und die Leistung Ihres Computers optimieren.

KAPITEL 7

Bereinigen Ihres Computers

Mit QuickClean können Sie Dateien und Ordner sicher löschen.

Wenn Sie im Internet surfen, kopiert Ihr Browser jede Internetseite und die darin enthaltenen Graphiken in einen Ordner im Zwischenspeicher auf Ihrer Festplatte. Der Browser kann die Seite dann schnell herunterladen, wenn Sie auf diese Seite zurückkehren. Das Zwischenspeichern von Dateien ist nützlich, wenn Sie wiederholt dieselben Internetseiten besuchen und sich ihr Inhalt nicht häufig ändert. Meistens sind die zwischengespeicherten Dateien jedoch nicht hilfreich und können gelöscht werden.

Sie können verschiedene Elemente mit den folgenden Cleanern löschen.

- Papierkorb-Cleaner: Leert Ihren Windows-Papierkorb.
- Cleaner für temporäre Dateien: Löscht Dateien, die in temporären Ordner gespeichert sind.
- Kurzbefehls-Cleaner: Löscht unterbrochene Kurzbefehle und Kurzbefehle mit einem verknüpften Programm.
- Cleaner für verlorene Dateifragmente: Löscht verlorene Dateifragmente von Ihrem Computer.
- Registrierungs-Cleaner: Löscht Windows-Registrierungsinformationen für Programme, die von Ihrem Computer gelöscht wurden.
- Cache Cleaner: Entfernt Dateien aus dem Zwischenspeicher, die beim Browsen im Internet anfallen. Dateien dieses Typs werden in der Regel als temporäre Internet-Dateien gespeichert.
- Cookie Cleaner: Löscht Cookies. Dateien dieses Typs werden in der Regel als temporäre Internet-Dateien gespeichert. Cookies sind kleine Dateien, die Ihr Webbrowser auf Anfrage eines Webservers auf Ihrem Computer speichert. Wenn Sie danach erneut eine Seite dieser Website vom Webserver laden, sendet Ihr Browser das Cookie zurück an den Webserver. Diese Cookies können wie Tags fungieren, mit denen der Webserver nachverfolgen kann, welche Seiten wie oft aufgerufen wurden.
- Browser-Verlaufs-Cleaner: Löscht Ihren Browser-Verlauf.
- Outlook Express und Outlook E-Mail Cleaner für gelöschte und gesendete Elemente: Löscht E-Mails aus Ihren Ordnern für gesendete und gelöschte Outlook-E-Mails.
- Cleaner für zuletzt verwendete Dateien: Löscht kürzlich verwendete Elemente, die auf Ihrem Computer gespeichert sind, wie Microsoft Office-Dokumente.

- ActiveX und Plugin Cleaner: Löscht ActiveX-Steuerelemente und -Plugins.
  ActiveX ist eine Technologie, die für die Implementierung von Steuerelementen in ein Programm verwendet wird. Ein ActiveX-Steuerlement kann eine Schaltfläche zur Oberfläche eines Programms hinzufügen. Die meisten dieser Steuerelemente sind harmlos. Einige Personen verwenden jedoch die ActiveX-Technologie, um Informationen von Ihrem Computer zu sammeln.
  Plugins sind kleine Softwareprogramme, die eine Verbindung zu größeren Anwendungen herzustellen, um weitere Funktionen verfügbar zu machen. Plugins ermöglichen es dem Webbrowser, auf Dateien zuzugreifen und diese auszuführen, die in HTML-Dokumente eingebettet sind, die Formate aufweisen, die der Browser normalerweise nicht erkennen würde (beispielsweise Animations-, Video- und Audiodateien).
- Cleaner für Systemwiederherstellungspunkte: Löscht alte Systemwiederherstellungspunkte von Ihrem Computer.

In diesem Kapitel

Verwenden von QuickClean 47

Verwenden von QuickClean

In diesem Abschnitt wird beschrieben, wie QuickClean verwendet wird.

Säubern Ihres Computers

Sie können nicht verwendete Dateien und Ordner löschen, Festplattenspeicher freigeben und die Leistung Ihres Computers optimieren.

So säubern Sie Ihren Computer:

1. Klicken Sie im Menü "Erweitert" auf **Tools**.
2. Klicken Sie auf **Computer warten**, und klicken Sie anschließend unter **McAfee QuickClean** auf **Start**.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Weiter**, um die in der Liste ausgewählten Standard-Cleaner zu übernehmen.
   - Wählen Sie die gewünschten Cleaner aus, und klicken Sie anschließend auf **Weiter.** Für den Cleaner für zuletzt verwendete Dateien können Sie auf **Eigenschaften** klicken, um die Programme zu löschen, deren Listen Sie nicht säubern möchten.
   - Klicken Sie auf **Standardwerte wiederherstellen**, um die Standard-Cleaner wiederherzustellen, und klicken Sie anschließend auf **Weiter**.
4. Klicken Sie nach Durchführung der Analyse auf **Weiter**, um das Löschen der Dateien zu bestätigen. Sie können diese Liste erweitern, um die Dateien anzuzeigen, die gesäubert werden, und deren Speicherort.
5. Klicken Sie auf **Weiter**.
6. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Weiter**, um den Standardwert **Nein, ich möchte meine Dateien mithilfe der Standardlöschung von Windows löschen** zu übernehmen.
   - Klicken Sie auf **Ja, ich möchte meine Dateien mit Shredder sicher löschen**, und geben Sie die Anzahl an Durchläufen an. Dateien, die mit Shredder gelöscht werden, können nicht wiederhergestellt werden.
7. Klicken Sie auf **Fertig stellen**.
8. Zeigen Sie unter **Zusammenfassung von QuickClean** die Anzahl an gelöschten Registrierungsdateien an sowie die Menge an Festplattenspeicher, der nach der Säuberung der Festplatte und der Internetdateien wieder zur Verfügug stand.

KAPITEL 8

McAfee Shredder

Gelöschte Dateien lassen sich auch nach dem Leeren des Papierkorbs wiederherstellen. Wenn eine Datei gelöscht wird, markiert Windows den betreffenden Speicherplatz auf dem Laufwerk als nicht mehr in Gebrauch, die Datei selbst ist jedoch noch vorhanden. Mit forensischen Computer-Tools können Steuererklärungen, Lebensläufe oder andere Dokumente, die von Ihnen gelöscht wurden, wiederhergestellt werden. Shredder schützt Ihre Privatsphäre, indem es unerwünschte Dateien permanent löscht.

Um eine Datei dauerhaft zu löschen, müssen Sie die vorhandene Datei wiederholt mit neuen Daten überschreiben. Microsoft(R) Windows löscht Dateien nicht sicher, da ansonsten sämtliche Dateivorgänge sehr langsam wären. Auch durch das Vernichten eines Dokuments wird nicht immer verhindert, dass das Dokument wiederhergestellt werden kann, da einige Programme temporäre verborgene Kopien geöffneter Dokumente erstellen. Wenn Sie nur die Dateien vernichten, die im Windows(R)-Explorer angezeigt werden, sind möglicherweise noch temporäre Kopien jener Dokumente irgendwo vorhanden.

Hinweis: Für vernichtete Dateien gibt es keine Sicherungskopien. Sie können von Shredder gelöschte Dateien nicht wiederherstellen.

In diesem Kapitel

Erläuterungen zu den Funktionen von Shredder 50
Vernichten unerwünschter Dateien mit Shredder ...51

Erläuterungen zu den Funktionen von Shredder

In diesem Abschnitt werden die Funktionen von Shredder beschrieben.

Funktionen

Shredder ermöglicht es Ihnen, den Inhalt Ihres Papierkorbs, temporäre Internetdateien, den Website-Verlauf, Dateien, Ordner und Datenträger wiederherzustellen.

KAPITEL 9

Vernichten unerwünschter Dateien mit Shredder

Shredder schützt Ihre persönlichen Daten, indem er unerwünschte Dateien, wie den Inhalt Ihres Papierkorbs, temporäre Internetdateien und den Website-Verlauf sicher und dauerhaft löscht. Sie können zu vernichtende Dateien und Ordner auswählen oder nach diesen suchen.

In diesem Kapitel

Verwenden von Shredder 52

Verwenden von Shredder

In diesem Abschnitt wird beschrieben, wie Shredder verwendet wird.

Vernichten von Dateien, Ordnern und Datenträgern

Dateien können auf Ihrem Computer verbleiben, auch nachdem Sie Ihren Papierkorb geleert haben. Wenn Sie jedoch Dateien vernichten, werden Ihre Daten dauerhaft gelöscht, und Hacker können nicht darauf zugreifen.

So vernichten Sie Dateien, Ordner und Datenträger:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Shredder**.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Dateien und Ordner löschen**, um Dateien und Ordner zu vernichten.
   - Klicken Sie auf **Die Daten eines ganzen Datenträgers löschen**, um einen Datenträger zu vernichten**.**
3. Wählen Sie eine der folgenden Vernichtungsstufen aus:
   - **Schnell**: Vernichtet die ausgewählten Elemente in einem Durchlauf.
   - **Umfassend**: Vernichtet die ausgewählten Elemente in sieben Durchläufen.
   - **Benutzerdefiniert**: Vernichtet die ausgewählten Elemente in bis zu zehn Durchläufen. Eine hohe Anzahl an Vernichtungsdurchläufen erhöht Ihre Stufe für die sichere Dateientfernung.
4. Klicken Sie auf **Weiter**.
5. Führen Sie einen der folgenden Vorgänge aus:
   - Wenn Sie Dateien vernichten, klicken Sie in der Liste **Zu vernichtende Dateien auswählen** auf **Inhalt des Papierkorbs**, **Temporäre Internet-Dateien** oder **Website-Verlauf**. Wenn Sie einen Datenträger vernichten möchten, klicken Sie auf den Datenträger.
   - Klicken Sie auf **Durchsuchen**, navigieren Sie zu den zu vernichtenden Dateien, und wählen Sie sie aus.
   - Geben Sie den Pfad zu den zu vernichtenden Dateien in der Liste **Zu vernichtende Dateien auswählen** ein.

6 Klicken Sie auf **Weiter**.

7 Klicken Sie auf **Fertig stellen**, um den Vorgang abzuschließen.

8 Klicken Sie auf **Fertig**.

KAPITEL 10

McAfee Network Manager

McAfee(R) Network Manager stellt eine graphische Ansicht der Computer und Komponenten dar, die Ihr Home-Netzwerk bilden. Sie können Network Manager verwenden, um den Schutzstatus jedes verwalteten Computers in Ihrem Netzwerk remote zu überwachen und gemeldete Sicherheitslücken auf diesen verwalteten Computern remote zu beheben.

Bevor Sie mit der Verwendung von Network Manager beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu Network Manager.

In diesem Kapitel

Funktionen 56
Erläuterung der Network Manager-Symbole 57
Erstellen eines verwalteten Netzwerks 59
Remote-Verwaltung des Netzwerks 69

Funktionen

Network Manager bietet die folgenden Funktionen:

Graphische Netzwerkzuordnung

Die Netzwerkzuordnung von Network Manager bietet eine graphische Übersicht des Sicherheitsstatus der Computer und der Komponenten, aus denen Ihr privates Netzwerk besteht. Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (wenn Sie beispielsweise einen Computer hinzufügen), erkennt die Netzwerkübersicht diese Änderungen. Sie können die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Komponenten der Netzwerkzuordnung anzeigen oder verbergen, um Ihre Ansicht anzupassen. Sie können auch die Details anzeigen, die mit den verschiedenen Komponenten verknüpft sind, die auf der Netzwerkzuordnung angezeigt werden.

Remote-Verwaltung

Verwenden Sie die Netzwerkübersicht von Network Manager zur Verwaltung des Sicherheitsstatus der Computer, aus denen Ihr privates Netzwerk besteht. Sie können einen Computer einladen, dem verwalteten Netzwerk beizutreten, den Schutzstatus des verwalteten Computers überwachen und bekannte Sicherheitslücken bei einem Remote-Computer im Netzwerk beheben.

Erläuterung der Network Manager-Symbole

Die folgende Tabelle erläutert die häufig auf der Network Manager-Netzwerkzuordnung verwendeten Symbole.

-Symbol	Beschreibung
	Steht für einen verwalteten Computer, der online ist.
	Steht für einen verwalteten Computer, der offline ist.
	Steht für einen unverwalteten Computer, auf dem die McAfee 2007-Sicherheits-Software installiert ist.
	Steht für einen unverwalteten Computer, der offline ist.
	Steht für einen Computer, der online ist und auf dem die McAfee 2007-Sicherheits-Software nicht installiert ist, oder für ein unbekanntes Netzwerkgerät.
	Steht für einen Computer, der offline ist und auf dem die McAfee 2007-Sicherheits-Software nicht installiert ist, oder für ein unbekanntes Netzwerkgerät, das offline ist.
	Bedeutet, dass das entsprechende Element geschützt und verbunden ist.
	Bedeutet, dass das entsprechende Element Ihrer Aufmerksamkeit bedarf.
	Bedeutet, dass das entsprechende Element Ihrer Aufmerksamkeit bedarf und keine Verbindung besteht.
	Steht für einen drahtlosen Home-Router.
	Steht für einen standardmäßigen Home-Router.
	Steht für das Internet, falls eine Verbindung besteht.
	Steht für das Internet, falls keine Verbindung besteht.

KAPITEL 11

Erstellen eines verwalteten Netzwerks

Sie erstellen ein verwaltetes Netzwerk, indem Sie mit den Elementen auf Ihrer Netzwerkzuordnung arbeiten und Mitglieder (Computer) zum Netzwerk hinzufügen.

In diesem Kapitel

Arbeiten mit der Netzwerkzuordnung.....60
Anmelden am verwalteten Netzwerk 63

Arbeiten mit der Netzwerkzuordnung

Jedes Mal, wenn Sie von einem Computer eine Verbindung zum Netzwerk herstellen, analysiert Network Manager den Status des Netzwerks, um festzustellen, ob Mitglieder vorliegen (verwaltet oder unverwaltet), welche Router-Attribute es gibt und wie der Internetstatus lautet. Wenn keine Mitglieder gefunden werden, nimmt Network Manager an, dass der derzeit verbundene Computer der erste Computer im Netzwerk ist, und macht den Computer automatisch zu einem verwalteten Mitglied mit Administratorrechten. Standardmäßig enthält der Name des Netzwerks den Arbeitsgruppen- oder Domänennamen des ersten Computers, auf dem die McAfee 2007-Sicherheits-Software installiert ist und der eine Verbindung zum Netzwerk herstellt. Sie können das Netzwerk jederzeit umbenennen.

Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (wenn Sie beispielsweise einen Computer hinzufügen), können Sie die Netzwerkmappe an Ihre Bedürfnisse anpassen. Sie können beispielsweise die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Komponenten der Netzwerkzuordnung anzeigen oder verbergen, um Ihre Ansicht anzupassen. Sie können auch die Details anzeigen, die mit den verschiedenen Komponenten verknüpft sind, die auf der Netzwerkzuordnung angezeigt werden.

Zugreifen auf die Netzwerkzuordnung

Sie können auf Ihre Netzwerkzuordnung zugreifen, indem Sie Network Manager über die SecurityCenter-Liste der häufigen Tasks starten. Die Netzwerkzuordnung bietet eine graphische Darstellung des Computers und der Komponenten, die Ihr Home-Netzwerk ausmachen.

So greifen Sie auf die Netzwerkzuordnung zu:

- Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
  Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.

Hinweis: Wenn Sie das erste Mal auf die Netzwerkübersicht zugreifen, werden Sie gefragt, ob die anderen Computern im Netzwerk vertrauenswürdig sind, bevor die Netzwerkübersicht angezeigt wird.

Netzwerkzuordnung aktualisieren

Sie können die Netzwerkzuordnung jederzeit aktualisieren, beispielsweise wenn ein anderer Computer dem verwalteten Netzwerk beitritt.

So aktualisieren Sie die Netzwerkzuordnung:

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
   Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.
2. Klicken Sie unter **Ich möchte** auf **Netzwerkzuordnung aktualisieren**.

Hinweis: Der Link **Netzwerkzuordnung aktualisieren** ist nur verfügbar, wenn in der Netzwerkzuordnung keine Elemente ausgewählt sind. Um die Auswahl eines Elements aufzuheben, klicken Sie auf das ausgewählte Element oder auf einen weißen Bereich in der Netzwerkzuordnung,

Netzwerk umbenennen

Standardmäßig enthält der Name des Netzwerks den Arbeitsgruppen- oder Domänennamen des ersten Computers, auf dem die McAfee 2007-Sicherheits-Software installiert ist und der eine Verbindung zum Netzwerk herstellt. Wenn dieser Name nicht passt, können Sie ihn ändern.

So benennen Sie das Netzwerk um:

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
   Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.
2. Klicken Sie unter **Ich möchte** auf **Netzwerk umbenennen**.
3. Geben Sie im Feld **Netzwerk umbenennen** den Namen des Netzwerks ein.
4. Klicken Sie auf **OK**.

Hinweis: Der Link **Netzwerk umbenennen** ist nur verfügbar, wenn in der Netzwerkzuordnung keine Elemente ausgewählt sind. Um die Auswahl eines Elements aufzuheben, klicken Sie auf das ausgewählte Element oder auf einen weißen Bereich in der Netzwerkzuordnung,

Anzeigen oder Verbergen von Elementen in der Netzwerkzuordnung

Standardmäßig werden alle Computer und Komponenten in Ihrem Home-Netzwerk in der Netzwerkzuordnung angezeigt. Wenn Sie jedoch Elemente ausgeblendet haben, können Sie sie jederzeit wieder anzeigen. Nur unverwaltete Elemente können ausgeblendet werden, verwaltete Computer können nicht ausgeblendet werden.

Ziel	Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Netzwerk verwalten**, und führen Sie anschließend die folgenden Schritte aus...
Verbergen eines Elements aus der Netzwerkzuordnung	Klicken Sie in der Netzwerkzuordnung auf ein Element, und klicken Sie anschließend unter **Ich möchte** auf **Dieses Element verbergen**. Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.
Anzeigen verborgener Elemente in der Netzwerkzuordnung	Klicken Sie unter **Ich möchte** auf **Verborgene Elemente anzeigen**.

Anzeigen der Elementdetails

Sie können detaillierte Informationen zu einer beliebigen Komponente in Ihrem Netzwerk anzeigen, indem Sie die Komponente in der Netzwerkzuordnung auswählen. Diese Informationen umfassen den Komponentennamen, seinen Schutzstatus und andere Informationen, die für die Verwaltung der Komponente erforderlich sind.

So zeigen Sie Details zu einem Element an:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Elements.
2. Zeigen Sie unter **Details** die Informationen zu diesem Element an.

Anmelden am verwalteten Netzwerk

Bevor ein Computer remote verwaltet wird oder ihm Zugriff auf die Remote-Verwaltung anderer Computer im Netzwerk gewährt werden kann, muss er ein vertrauenswürdiges Mitglied des Netzwerks werden. Die Netzwerkmitgliedschaft wird neuen Computern von bestehenden Netzwerkmitgliedern (Computern) mit Administratorrechten gewährt. Um sicherzustellen, dass sich nur vertrauenswürdige Computer am Netzwerk anmelden, müssen sowohl Benutzer des gewährenden als auch des anzumeldenden Computers sich gegenseitig authentifizieren.

Wenn ein Computer dem Netzwerk beitritt, wird er aufgefordert, seinen McAfee-Schutzstatus für die anderen Computer im Netzwerk sichtbar zu machen. Wenn ein Computer zustimmt und seinen Schutzstatus sichtbar macht, wird er ein *verwaltetes* Mitglied des Netzwerks. Wenn ein Computer ablehnt und seinen Schutzstatus nicht sichtbar macht, wird er ein *unverwaltetes* Mitglied des Netzwerks. Unverwaltete Mitglieder des Netzwerks sind normalerweise Gastcomputer, die Zugriff auf andere Netzwerkfunktionen erlangen möchten (z. B. auf die Datei- oder Druckerfreigabe).

Hinweis: Wenn Sie andere Netzwerkprogramme von McAfee installiert haben (z. B. McAfee Wireless Network Security oder EasyNetwork), wird der Computer nach dem Beitritt auch in diesen Programmen als verwalteter Computer erkannt. Die Berechtigungsstufe, die einem Computer in Network Manager zugewiesen wird, gilt für alle McAfee-Netzwerkprogramme. Weitere Informationen dazu, was Gastberechtigungen, vollständige oder administrative Berechtigungen in anderen McAfee-Netzwerkprogrammen bedeuten, finden Sie in der Dokumentation zu dem jeweiligen Programm.

Anmelden an einem verwalteten Netzwerk

Wenn Sie eine Einladung erhalten, einem verwalteten Netzwerk beizutreten, können Sie diese entweder annehmen oder ablehnen. Sie können auch bestimmen, ob Sie möchten, dass dieser und andere Computer im Netzwerk gegenseitig ihre Sicherheitseinstellungen überwachen (beispielsweise ob die Virenschutzdienste eines Computers auf dem neuesten Stand sind).

So melden Sie sich an einem verwalteten Netzwerk an:

1. Aktivieren Sie im Dialogfeld für die Einladung das Kontrollkästchen **Es diesem und anderen Computern erlauben, gegenseitig ihre Sicherheitseinstellungen zu überwachen**, um es anderen Computern im verwalteten Netzwerk zu erlauben, die Sicherheitseinstellungen Ihres Computers zu überwachen.
2. Klicken Sie auf **Anmelden**.
   Wenn Sie die Einladung annehmen, werden zwei Spielkarten angezeigt.
3. Bestätigen Sie, dass die Spielkarten dieselben sind wie diejenigen, die auf dem Computer angezeigt werden, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden.
4. Klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Anmelden am Netzwerk ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Einladen eines Computers, sich am verwalteten Netzwerk anzumelden

Wenn ein Computer dem verwalteten Netzwerk hinzugefügt wird oder ein anderer unverwalteter Computer im Netzwerk vorliegt, können Sie diesen Computer einladen, sich am verwalteten Netzwerk anzumelden. Nur Computer mit Administratorrechten für das Netzwerk können andere Computer dazu einladen, sich am Netzwerk anzumelden. Wenn Sie die Einladung senden, können Sie auch die Berechtigungsstufe angeben, die Sie dem anzumeldenden Computer zuweisen möchten.

So laden Sie einen Computer ein, sich am verwalteten Netzwerk anzumelden:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines unverwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.
3. Klicken Sie im Dialogfeld "Einen Computer einladen, diesem verwalteten Netzwerk beizutreten" auf eine der folgenden Optionen:
   - **Zugriff als Gast gewähren**
     Der Gastzugriff erlaubt dem Computer den Zugriff auf das Netzwerk.
   - **Vollständigen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**
     Mit dem vollständigen Zugriff (wie mit dem Gastzugriff) können Computer auf das Netzwerk zugreifen.
   - **Administrativen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**
     Mit dem administrativen Zugriff können Computer mit Administratorrechten auf das Netzwerk zugreifen. Dieser Zugriff erlaubt es dem Computer außerdem, anderen Computern Zugriff zu gewähren, die sich am verwalteten Netzwerk anmelden möchten.

4 Klicken Sie auf **Einladen**.
Es wird eine Einladung, dem verwalteten Netzwerk beizutreten, an den Computer gesendet. Wenn der Computer die Einladung annimmt, werden zwei Spielkarten angezeigt.

5 Bestätigen Sie, dass die Spielkarten dieselben sind wie diejenigen, die auf dem Computer angezeigt werden, den Sie eingeladen haben, sich am verwalteten Netzwerk anzumelden.

6 Klicken Sie auf **Zugriff gewähren**.

Hinweis: Wenn der Computer, den Sie eingeladen haben, sich am verwalteten Netzwerk anzumelden, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Wenn Sie es dem Computer erlauben, sich am Netzwerk anzumelden, werden dadurch andere Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Zugriff verweigern**.

Computer im Netzwerk nicht mehr als vertrauenswürdig einstufen

Wenn Sie fälschlicherweise zustimmen, den anderen Computern im Netzwerk zu vertrauen, so können Sie diese Auswahl auch wieder aufheben.

So erklären Sie Computer in diesem Netzwerk als nicht mehr vertrauenswürdig:

- Klicken Sie unter **Ich möchte** auf **Computern in diesem Netzwerk nicht mehr vertrauen**.

Hinweis: Der Link **Computern in diesem Netzwerk nicht mehr vertrauen** ist nur verfügbar, wenn sich keine anderen verwalteten Computer am Netzwerk angemeldet haben.

KAPITEL 12

Remote-Verwaltung des Netzwerks

Nachdem Sie Ihr verwaltetes Netzwerk eingerichtet haben, können Sie Network Manager verwenden, um die Computer und Komponenten, die sich in Ihrem Netzwerk befinden, remote zu verwalten. Sie können den Status und die Berechtigungsstufen der Computer und Komponenten überwachen und Sicherheitslücken remote beheben.

In diesem Kapitel

Überwachen des Status und der Berechtigungen 70
Beheben von Sicherheitslücken.....73

Überwachen des Status und der Berechtigungen

Ein verwaltetes Netzwerk hat zwei Arten von Mitgliedern: verwaltete Mitglieder und unverwaltete Mitglieder. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren McAfee-Schutzstatus einzusehen, unverwaltete Mitglieder tun das nicht. Unverwaltete Mitglieder sind normalerweise Gastcomputer, die Zugriff auf andere Netzwerkfunktionen erlangen möchten (z. B. auf die Datei- und Druckerfreigabe). Ein unverwalteter Computer kann jederzeit von einem anderen verwalteten Computer im Netzwerk eingeladen werden, ein verwalteter Computer zu werden. Ebenso kann ein verwalteter Computer jederzeit ein unverwalteter Computer werden.

Verwalteten Computern sind entweder administrative, vollständige oder Gastberechtigungen zugewiesen. Administrative Berechtigungen erlauben es dem verwalteten Computer, den Schutzstatus aller anderen verwalteten Computer im Netzwerk zu verwalten und anderen Computern die Mitgliedschaft im Netzwerk zu gewähren. Vollständige und Gastberechtigungen erlauben es einem Computer nur, auf das Netzwerk zuzugreifen. Sie können die Berechtigungsstufe eines Computers jederzeit ändern.

Da ein verwaltetes Netzwerk auch aus Geräten besteht (z. B. Routern), können Sie Network Manager auch für die Verwaltung dieser Geräte verwenden. Sie können auch die Anzeigeeigenschaften eines Geräts in der Netzwerkzuordnung konfigurieren und verändern.

Überwachen des Schutzstatus eines Computers

Wenn der Schutzstatus eines Computers nicht im Netzwerk überwacht wird (entweder, weil der Computer kein Mitglied des Netzwerks ist, oder weil der Computer ein unverwaltetes Mitglied des Netzwerks ist), können Sie eine Anfrage für die Überwachung stellen.

So überwachen Sie den Schutzstatus eines Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines unverwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.

Stoppen der Überwachung des Schutzstatus eines Computers

Sie können die Überwachung des Schutzstatus eines verwalteten Computers in Ihrem privaten Netzwerk stoppen. Der Computer wird dann zu einem unverwalteten Computer.

So stoppen Sie die Überwachung des Schutzstatus eines Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines verwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer nicht mehr überwachen**.
3. Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.

Ändern der Berechtigungen eines verwalteten Computers

Sie können die Berechtigungen eines verwalteten Computers jederzeit ändern. Dadurch können Sie angeben, welche Computer den Schutzstatus (Sicherheitseinstellungen) anderer Computer im Netzwerk überwachen können.

So ändern Sie die Berechtigungen eines verwalteten Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines verwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Berechtigungen für diesen Computer ändern**.
3. Aktivieren oder Deaktivieren Sie im Dialogfeld zum Ändern der Berechtigungen das Kontrollkästchen, das angibt, ob dieser Computer und andere Computer im verwalteten Netzwerk den Schutzstatus der anderen Computer überwachen können.
4. Klicken Sie auf **OK**.

Verwalten eines Geräts

Sie können ein Gerät verwalten, indem Sie von Network Manager aus auf ihre Verwaltungs-Website zugreifen.

So verwalten Sie ein Gerät:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Geräts.
2. Klicken Sie unter **Ich möchte** auf **Dieses Gerät verwalten**. Es wird ein Webbrowser geöffnet, der die Verwaltungs-Webseite des Geräts anzeigt.
3. Geben Sie in Ihrem Webbrowser Ihre Anmeldeinformationen ein, und konfigurieren Sie die Sicherheitseinstellungen des Geräts.

Hinweis: Wenn es sich bei dem Gerät um einen durch Wireless Network Security geschützten drahtlosen Router oder Zugriffspunkt handelt, müssen Sie Wireless Network Security verwenden, um die Sicherheitseinstellungen eines Geräts zu konfigurieren.

Ändern der Anzeigeeigenschaften eines Geräts

Wenn Sie die Anzeigeeigenschaften eines Geräts verändern, können Sie den Anzeigenamen eines Geräts in der Netzwerkzuordnung ändern und angeben, ob es sich bei diesem Gerät um einen drahtlosen Router handelt.

So ändern Sie die Anzeigeeigenschaften eines Geräts:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Geräts.
2. Klicken Sie unter **Ich möchte** auf **Geräteeigenschaften ändern**.
3. Um den Anzeigenamen des Geräts anzugeben, geben Sie einen Namen in das Feld **Name** ein.
4. Zum Angeben des Gerätetyps klicken Sie auf eine der folgenden Optionen:
   - **Router**
     Diese Option steht für einen standardmäßigen Home-Router.
   - **Drahtloser Router**
     Diese Option steht für einen drahtlosen Home-Router.
5. Klicken Sie auf **OK**.

Beheben von Sicherheitslücken

Verwaltete Computer mit Administratorrechten können den McAfee-Schutzstatus anderer verwalteter Computer im Netzwerk überwachen und sämtliche gemeldeten Sicherheitslücken remote beheben. Wenn beispielweise der McAfee-Schutzstatus eines verwalteten Computers angibt, dass VirusScan deaktiviert ist, kann ein anderer verwalteter Computer mit Administratorrechten diese Sicherheitslücke *beheben*, indem er VirusScan remote aktiviert.

Wenn Sie Sicherheitslücken remote beheben, repariert Network Manager automatisch die meisten gemeldeten Probleme. Einige Sicherheitslücken erfordern jedoch möglicherweise ein manuelles Eingreifen auf dem lokalen Computer. In diesem Fall behebt Network Manager diejenigen Probleme, die remote repariert werden können, und fordert Sie dann auf, die übrigen Probleme zu beheben, indem Sie sich auf dem betreffenden Computer bei SecurityCenter anmelden und die angegebenen Empfehlungen befolgen. In einigen Fällen lautet der Vorschlag, dass die McAfee 2007-Sicherheits-Software auf dem Remote-Computer oder den Computern in Ihrem Netzwerk installiert werden sollte.

Sicherheitslücken schließen

Sie können Network Manager verwenden, um automatisch die meisten Sicherheitslücken auf verwalteten Remote-Computern zu beheben. Wenn beispielsweise VirusScan auf einem Remote-Computer deaktiviert ist, können Sie für die automatische Aktivierung Network Manager verwenden.

So beheben Sie Sicherheitslücken:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Elements.
2. Zeigen Sie unter **Details** den Schutzstatus eines Elements an.
3. Klicken Sie unter **Ich möchte** auf **Sicherheitslücken schließen**.
4. Klicken Sie auf **OK**, nachdem die Sicherheitslücken geschlossen wurden.

Hinweis: Auch wenn Network Manager die meisten Sicherheitslücken automatisch schließt, erfordert das Beheben einiger Probleme möglicherweise das Starten von SecurityCenter auf dem betroffenen Computer und das Befolgen der angegebenen Empfehlungen.

Installieren der McAfee-Sicherheits-Software auf Remote-Computern

Wenn auf einem oder meheren Computern in Ihrem Netzwerk die McAfee 2007-Sicherheits-Software nicht ausgeführt wird, kann ihr Schutzstatus nicht remote überwacht werden. Wenn Sie diese Computer remote überwachen möchten, müssen Sie zu jedem Computer gehen und die McAfee 2007-Sicherheits-Software installieren.

So installieren Sie die McAfee-Sicherheits-Software auf einem Remote-Computer:

1. Besuchen Sie in einem Browser auf dem Remote-Computer die Seite http://download.mcafee.com/us/.
2. Befolgen Sie die Bildschirmanweisungen für die Installation der McAfee 2007-Sicherheits-Software auf dem Computer.

KAPITEL 13

McAfee Wireless Network Security

Wireless Network Security bietet eine intuitive Benutzeroberfläche und aktuellen automatischen Schutz vor Datendiebstahl, unerlaubtem Netzwerkzugriff und Breitband-Downloads durch Eindringlinge. Das Programm verschlüsselt Ihre persönlichen Daten bei der Übertragung über Wi-Fi und verhindert, dass Hacker auf Ihr drahtloses Netzwerk zugreifen.

Wireless Network Security verhindert durch die folgenden Maßnahmen, dass Hacker Ihr drahtloses Netzwerk angreifen:

- Verhinderung nicht autorisierter Verbindungen zum Wi-Fi-Netzwerk,
- Verhinderung des Abfangens von Daten, die über ein Wi-Fi-Netzwerk übertragen werden,
- Erkennen von Verbindungsversuchen zu einem Wi-Fi-Netzwerk.

Wireless Network Security kombiniert benutzerfreundliche Funktionen, wie beispielsweise eine sofortige Netzwerksperre und das schnelle Hinzufügen legitimer Benutzer zum Netzwerk, mit robusten Sicherheitsfunktionen, wie beispielsweise automatische Schlüsselerstellung und planmäßige Schlüsselrotation.

In diesem Kapitel

Funktionen 76
Wireless Network Security starten 78
Drahtlose Netzwerke schützen 81
Drahtlosen Netzwerken verwalten 99
Sicherheit für drahtloses Netzwerk verwalten 113
Drahtlose Netzwerke überwachen..... 129

Funktionen

Wireless Network Security bietet die folgenden Funktionen:

Ständig aktiver Schutz

Wireless Network Security erkennt und schützt automatisch gefährdete drahtlose Netzwerke, zu denen Sie eine Verbindung herstellen.

Leicht verständliche Benutzeroberfläche

Ermöglicht Ihnen den Schutz des Netzwerks, ohne dass Sie schwierige Entscheidungen treffen oder komplizierte technische Begriffe kennen müssen.

Starke automatische Verschlüsselung

Gewährt ausschließlich Familienangehörigen und Freunden Zugriff auf das Netzwerk und schützt Ihre Daten bei der Übertragung.

Reine Softwarelösung

Wireless Network Security funktioniert mit einem herkömmlichen drahtlosen Router oder Zugriffspunkt und mit normaler Sicherheitssoftware. Sie müssen keine zusätzliche Hardware erwerben.

Automatische Schlüsselrotation

Selbst die entschlossensten Hacker können Ihre Daten nicht abfangen, da der Schlüssel ständig geändert wird.

Hinzufügen von Netzwerkbenutzern

Sie können Ihren Familienangehörigen und Freunden mühelos Zugriff auf das Netzwerk gewähren. Sie können Benutzer drahtlos oder mittels Übertragungssoftware über ein USB-Laufwerk hinzufügen.

Intuitives Verbindungs-Tool

Das Tool für drahtlose Verbindungen ist intuitiv zu bedienen und informativ. Es zeigt Details zur Signalstärke und zum Sicherheitsstatus an.

Ereignisprotokollierung und Warnungen

Leicht verständliche Berichte und Warnungen bieten erfahrenen Benutzern weitere Informationen zum drahtlosen Netzwerk.

Aussetzmodus

Hiermit können Sie die Schlüsselrotation vorübergehend aussetzen, damit bestimmte Anwendungen ohne Unterbrechung ausgeführt werden können.

Kompatibilität mit anderer Hardware

Wireless Network Security aktualisiert sich selbst automatisch mit den neuesten Modulen für drahtlose Router oder Zugriffspunkte der am häufigsten verwendeten Marken. Dazu gehören: Linksys(R), NETGEAR(R), D-Link(R), Belkin(R), TRENDnet(R) und andere.

Wireless Network Security starten

Nach der Installation wird Wireless Network Security automatisch aktiviert. Ein manuelles Starten ist nicht notwendig. Optional können Sie drahtlosen Schutz auch manuell aktivieren und deaktivieren.

Nach der Installation von Wireless Network Security versucht Ihr Computer automatisch, eine Verbindung zum drahtlosen Router aufzubauen. Nachdem die Verbindung aufgebaut wurde, programmiert der Computer den Verschlüsselungsschlüssel in den drahtlosen Router. Wenn das Standardkennwort geändert wurde, erfolgt eine Kennwortabfrage, damit Wireless Network Security den drahtlosen Router mit dem gemeinsamen Verschlüsselungsschlüssel und einem hohen Sicherheitsmodus konfigurieren kann. Ihr Computer wird ebenfalls mit demselben freigegebenen Schlüssel und dem Verschlüsselungsmodus konfiguriert, wodurch eine sichere drahtlose Verbindung aufgebaut wird.

Wireless Network Security starten

Wireless Network Security ist standardmäßig aktiviert. Sie können drahtlosen Schutz allerdings auch manuell aktivieren und deaktivieren.

Die Aktivierung des drahtlosen Schutzes schützt Ihr drahtloses Netzwerk vor Intrusionen und Datenabfang. Besteht jedoch eine Verbindung mit einem externen drahtlosen Netzwerk, variiert Ihr Schutz in Abhängigkeit von der Sicherheitsebene.

So aktivieren Sie den drahtlosen Schutz manuell:

1. Führen Sie im Bereich "McAfee SecurityCenter" einen der folgenden Schritte aus:
   - Wählen Sie **Internet & Netzwerk**, und klicken Sie dann auf **Konfigurieren**.
   - Wählen Sie das Menü **Erweitert**, und dann im Bereich **Startseite** die Option **Konfigurieren**. Zeigen Sie auf **Internet & Netzwerk**.
2. Klicken Sie im Bereich **Internet & Netzwerkkonfiguration** unter **Drahtloser Schutz** auf **Ein**.

Hinweis: Wenn ein kompatibler drahtloser Adapter installiert ist, wird Wireless Network Security automatisch aktiviert.

Wireless Network Security deaktivieren

Wireless Network Security ist standardmäßig aktiviert. Sie können drahtlosen Schutz allerdings auch manuell aktivieren und deaktivieren.

Durch die Deaktivierung des drahtlosen Schutzes ist Ihr Netzwerk Intrusionen und Datenabfang schutzlos ausgeliefert.

So deaktivieren Sie den drahtlosen Schutz:

1. Führen Sie im Bereich "McAfee SecurityCenter" einen der folgenden Schritte aus:
   - Wählen Sie **Internet & Netzwerk**, und klicken Sie dann auf **Konfigurieren**.
   - Wählen Sie das Menü **Erweitert** und dann im Bereich **Startseite** die Option **Konfigurieren**. Zeigen Sie auf **Internet & Netzwerk**.
2. Klicken Sie im Bereich **Internet & Netzwerkkonfiguration** unter **Drahtloser Schutz** auf **Aus**.

KAPITEL 14

Drahtlose Netzwerke schützen

Wireless Network Security schützt Ihr Netzwerk durch die Einbindung drahtloser Verschlüsselung (entweder durch WEP, WPA oder WPA2, je nachdem, welche Ausstattung Sie haben). Es programmiert die Clients und drahtlosen Router automatisch mit den gültigen Verschlüsselungsschlüsseldaten, sodass der drahtlose Router Verbindungsautorisierungen für Computer erteilen kann. Drahtlose Netzwerke, die durch Verschlüsselung geschützt sind, sperren den Zugriff nicht autorisierter Benutzer auf das drahtlose Netzwerk. Weiterhin werden die Daten, die über ein drahtloses Netzwerk übertragen werden, geschützt. Wireless Network Security erreicht dies durch die folgenden Maßnahmen:

- Erstellung und Verteilung eines langen, starken, zufälligen und gemeinsamen Verschlüsselungsschlüssels,
- Planmäßiges Rotieren des Verschlüsselungsschlüssels,
- Konfiguration aller drahtlosen Geräte mit Verschlüsselungsschlüsseln.

In diesem Kapitel

Geschützte drahtlose Netzwerke einrichten 82
Computer zum geschützten drahtlosen Netzwerk hinzufügen 95

Geschützte drahtlose Netzwerke einrichten

Wenn Wireless Network Security installiert ist, erfolgt eine automatische Aufforderung zur Sicherung des unsicheren drahtlosen Netzwerks, mit dem Sie verbunden sind, oder zur Anmeldung an einem zuvor geschützten drahtlosen Netzwerk.

Wenn Sie nicht mit einem drahtlosen Netzwerk verbunden sind, sucht Wireless Network Security nach einem durch McAfee geschützten Netzwerk mit hoher Signalstärke und fordert den Benutzer auf, sich an diesem Netzwerk anzumelden. Sollten keine geschützten Netzwerke zur Verfügung stehen, sucht Wireless Network Security nach unsicheren Netzwerken mit starken Signalen. Wenn eines gefunden wurde, werden Sie aufgefordert, dieses Netzwerk zu schützen.

Alle drahtlosen Netzwerke, die nicht durch McAfee Wireless Network Security geschützt sind, werden von McAfee als "nicht geschützt" angesehen, auch wenn diese drahtlose Sicherheitsmechanismen, wie beispielsweise WEP und WPA, verwenden.

Alle drahtlosen Netzwerke, die nicht durch Wireless Network Security geschützt sind, werden von McAfee als nicht geschützt angesehen, auch wenn diese drahtlose Sicherheitsmechanismen, wie beispielsweise WEP und WPA, verwenden.

Über Zugriffstypen

Jeder drahtlose Computer, auf dem Wireless Network Security installiert ist, kann ein geschütztes drahtloses Netzwerk erstellen. Der erste Computer, der einen Router schützt und ein geschütztes drahtloses Netzwerk erstellt, erhält automatisch administrativen Zugriff auf dieses Netzwerk. Ein bestehender Benutzer mit administrativen Zugriffsrechten kann Computern, die sich später anmelden, administrative, vollständige oder Gast-Zugriffsrechte erteilen.

Computer mit administrativen oder vollständigen Zugriffstypen können die folgenden Aufgaben durchführen:

- Schutz und Entfernen eines Routers oder Zugriffspunkts,
- Rotieren von Sicherheitsschlüsseln,
- Ändern von Netzwerk-Sicherheitseinstellungen,
- Netzwerkreparaturen,
- Erteilung für Zugriffsberechtigungen für Computer auf das Netzwerk,
- Aufhebung von Zugriffsberechtigungen zum geschützten drahtlosen Netzwerk,
- Änderung der Administratorstufe eines Computers.

Computer mit Gast-Zugriffstypen können die folgenden Aufgaben durchführen:

- Herstellen einer Verbindung zu einem Netzwerk,
- Anmeldung an einem Netzwerk,
- Änderung von Einstellungen, die spezifisch für den Gastcomputer sind.

Hinweis: Computer können an einem drahtlosen Netzwerk über administrative Zugriffsrechte und an einem anderen über Gast- oder vollständige Zugriffsrechte verfügen. Ein Computer, der über Gast- oder vollständige Zugriffsrechte auf ein Netzwerk verfügt, kann ein neues Netzwerk erstellen.

Verwandte Themen

- Anmelden an einem geschützten drahtlosen Netzwerk (Seite 86)
- Computern administrativen Zugriff gewähren (Seite 92)
- Netzwerkzugriffsrechte aufheben (Seite 111)

Geschützte drahtlose Netzwerke erstellen

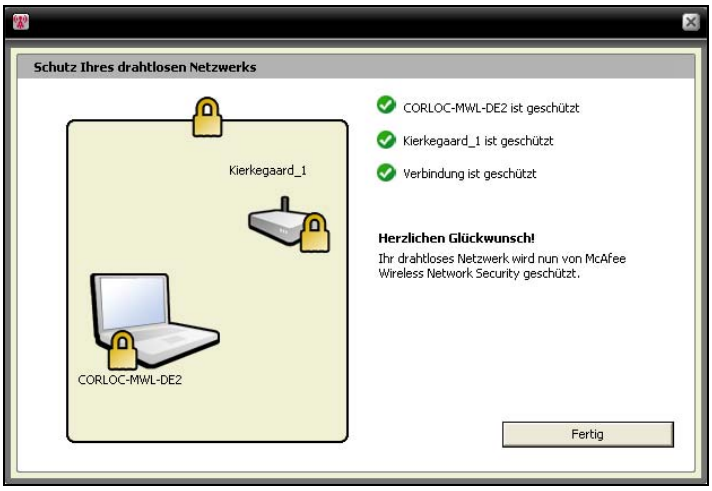
Um ein geschütztes drahtloses Netzwerk zu erstellen, müssen Sie zunächst den drahtlosen Router oder Zugriffspunkt des drahtlosen Netzwerks hinzufügen.

So fügen Sie einen drahtlosen Router oder Zugriffspunkt hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Drahtlosen Router/Zugriffspunkt schützen** auf **Schützen**.
4. Wählen Sie im Bereich "Drahtlosen Router/Zugriffspunkt schützen" ein drahtloses Netzwerk aus, das geschützt werden soll und klicken Sie auf **Schützen**.

Das Fenster "Schutz Ihres drahtlosen Netzwerks" wird geöffnet, während Wireless Network Security versucht, Ihren Computer, Router und die Netzwerkverbindung zu schützen.

Ein erfolgreicher Schutz all dieser Komponenten hat den gesamten Schutz Ihres drahtlosen Netzwerks zur Folge.



5 Klicken Sie auf **Fertig**.

Hinweis: Nach dem Schutz eines Netzwerks erinnert das Dialogfenster "Ihr nächster Schritt" daran, dass Sie Wireless Network Security auf allen drahtlosen Computern installieren müssen, damit diese sich am Netzwerk anmelden können.

Wenn Sie zuvor für Ihren Router oder Zugriffspunkt einen vorinstallierten Schlüssel manuell konfiguriert haben und keine Verbindung bestand, während Sie versuchten, den Router oder Zugriffspunkt zu schützen, müssen Sie den Schlüssel auch in das Feld für den WEP-Schlüssel eingeben und auf "Verbinden" klicken. Wenn Sie zuvor den administrativen Benutzernamen oder das Kennwort geändert haben, erfolgt eine Aufforderung zur Eingabe dieser Informationen, bevor ein Router oder Zugriffspunkt geschützt wird.

Verwandte Themen

- Schutz anderer drahtloser Geräte (Seite 93)
- Computer zum geschützten drahtlosen Netzwerk hinzufügen (Seite 95)

An geschützten drahtlosen Netzwerken anmelden

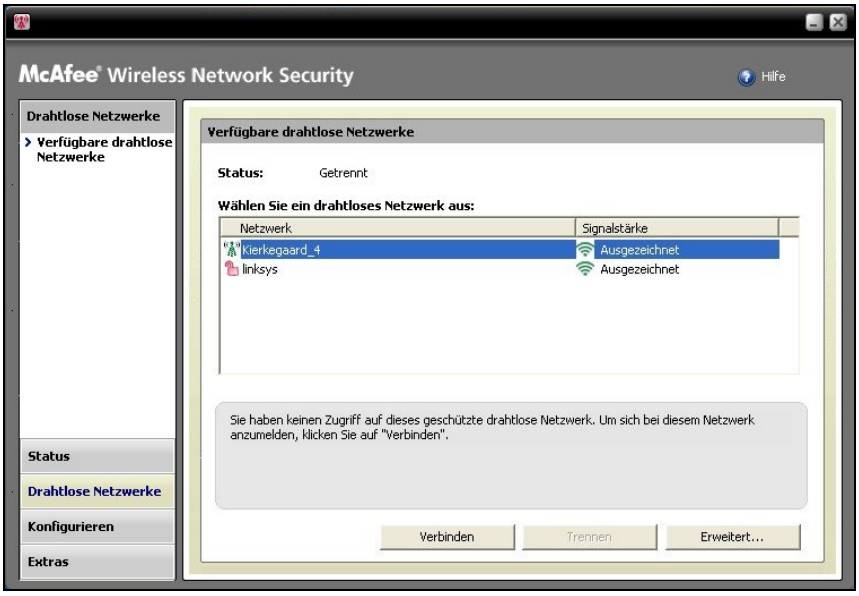
Ein geschütztes Netzwerk verhindert, dass Hacker Daten abfangen, die über das Netzwerk übertragen werden, und eine Verbindung zu Ihrem Netzwerk herstellen. Bevor ein berechtigter Computer auf ein geschütztes drahtloses Netzwerk zugreifen kann, muss dieser zunächst angemeldet werden.

Wenn ein Computer die Anmeldung zu einem verwalteten Netzwerk anfragt, wird eine Nachricht an die anderen Computer des Netzwerks gesendet, die über administrative Zugriffsrechte verfügen. Als Administrator sind Sie dafür zuständig, zu entscheiden, welche Art von Zugriffsrecht einem Computer gewährt wird: als Gast, vollständig oder administrativ.

Bevor Sie sich an einem geschützten Netzwerk anmelden können, müssen Sie Wireless Network Security installieren und dann eine Verbindung zum geschützten drahtlosen Netzwerk aufbauen. Ein bestehender Netzwerkbenutzer, der über administrative Zugriffsrechte auf das geschützte drahtlose Netzwerk verfügt, muss Ihre Anmeldung zum Netzwerk genehmigen. Nach der Anmeldung zum Netzwerk ist bei einem Neuaufbau der Verbindung keine Neuanmeldung erforderlich. Sowohl der Rechtegewährer als auch der sich Anmeldende müssen über eine aktive drahtlose Verbindung verfügen. Der Rechtegewährer muss ein Administratorcomputer sein, der mit dem Netzwerk verbunden ist.

So melden Sie sich an einem geschützten drahtlosen Netzwerk an:

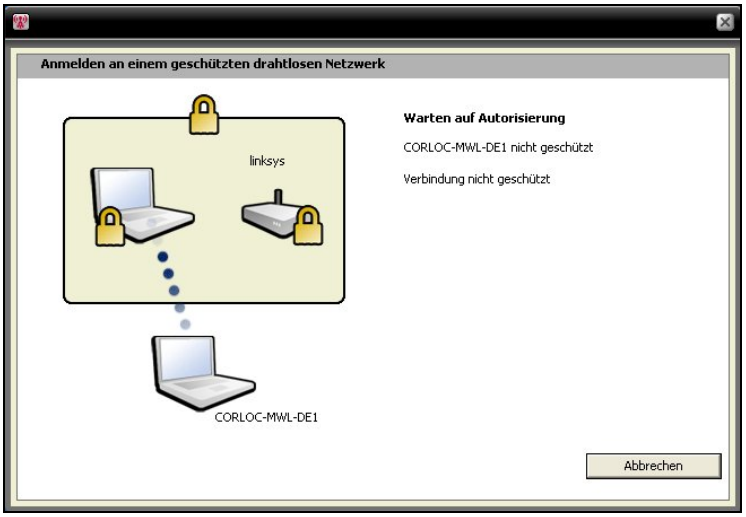
1. Klicken Sie auf dem ungeschützten Computer mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Wählen Sie im Bereich "Verfügbare drahtlose Netzwerke" ein Netzwerk aus und klicken Sie auf **Verbinden**.



4 Klicken Sie im Dialogfenster "Beim geschützten drahtlosen Netzwerk anmelden" auf **Ja**, um sich am Netzwerk anzumelden.

Beim geschützten drahtlosen Netzwerk anmelden
Das Netzwerk Kierkegaard_4 wird von McAfee Wireless Network Security geschützt.
Um sich bei diesem Netzwerk anzumelden, klicken Sie auf "Ja".
Ja
Nein

Während Wireless Network Security versucht, die Genehmigung für die Anmeldung zum Netzwerk zu erhalten, erscheint das Fenster "Anmelden an einem geschützten drahtlosen Netzwerk" auf dem Computer, der versucht, sich am Netzwerk anzumelden.



5 Auf dem Administratorcomputer, über den die Gast-, vollständigen und administrativen Zugriffsrechte gewährt werden, erscheint das Fenster "Am Netzwerk anmelden".

Achtung! Ein Computer möchte sich am Netzwerk anmelden.
Verwaltetes Netzwerk - linksys
CORLOC_JIXP versucht, sich am Netzwerk linksys anzumelden.
Wenn Sie diesen Computer nicht kennen, empfehlen wir Ihnen, auf Anfrage ignorieren zu klicken. Wählen Sie anderenfalls den zu autorisierenden Zugriffstyp aus, und klicken Sie auf Zugriff gewähren .
CORLOC_JIXP den folgenden Zugriff gewähren:
Zugriff als Gast gewähren
Vollständigen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren
Administrativen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren
Hilfe
Zugriff gewähren
Anfrage ignorieren

Wählen Sie im Dialogfenster "Am Netzwerk anmelden" eine der folgenden Optionen aus:

Zugriff als Gast gewähren	Diese Option erlaubt dem Computer, Dateien an andere auf dem drahtlosen Netzwerk befindliche Computer zu senden. Der Datenaustausch mit McAfee EasyNetwork ist nicht möglich.
Vollständigen Zugriff auf alle verwalteten Netzwerk-anwendungen gewähren	Diese Option erlaubt dem Computer den Datenversand an und den Datenaustausch mit McAfee EasyNetwork.
Administrativen Zugriff auf alle verwalteten Netzwerk-anwendungen gewähren:	Diese Option erlaubt dem Computer den Datenversand an und den Datenaustausch mit McAfee EasyNetwork, die Erteilung von Zugriffsrechten für andere Computer und die Anpassung der Zugriffsstufen der anderen Computer auf dem drahtlosen Netzwerk.

6 Klicken Sie auf **Zugriff gewähren**.

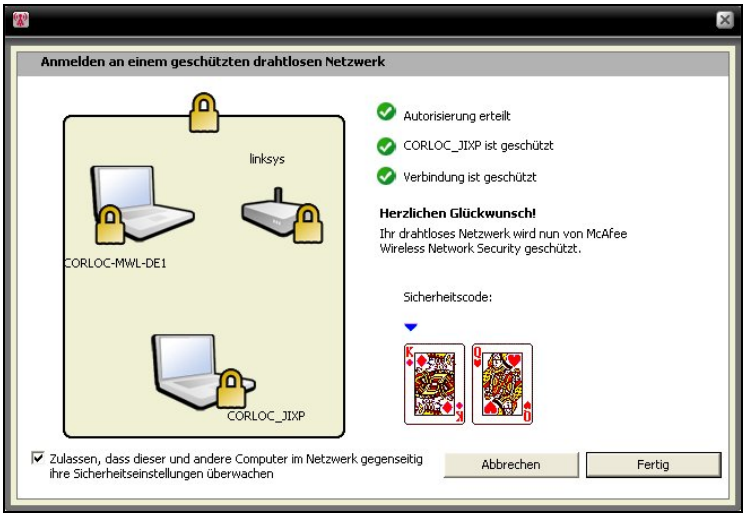
7 Bestätigen Sie, dass die im Bereich "Gewähren von Netzwerkzugriff" angezeigten Karten denen auf dem Computer angezeigten entsprechen, der versucht, sich am drahtlosen Netzwerk anzumelden. Sollten die Karten übereinstimmen, klicken Sie auf **Zugriff gewähren**.

Sollten die Computer nicht die gleichen Spielkarten anzeigen, liegt möglicherweise ein Sicherheitsverstoß vor. Diesem

Computer Zugriffsrechte zum Netzwerk zu gewähren, kann ein Risiko für Ihren Computer darstellen. Um dem Computer den Zugriff auf das drahtlose Netzwerk zu untersagen, klicken Sie auf **Zugriff verweigern**.

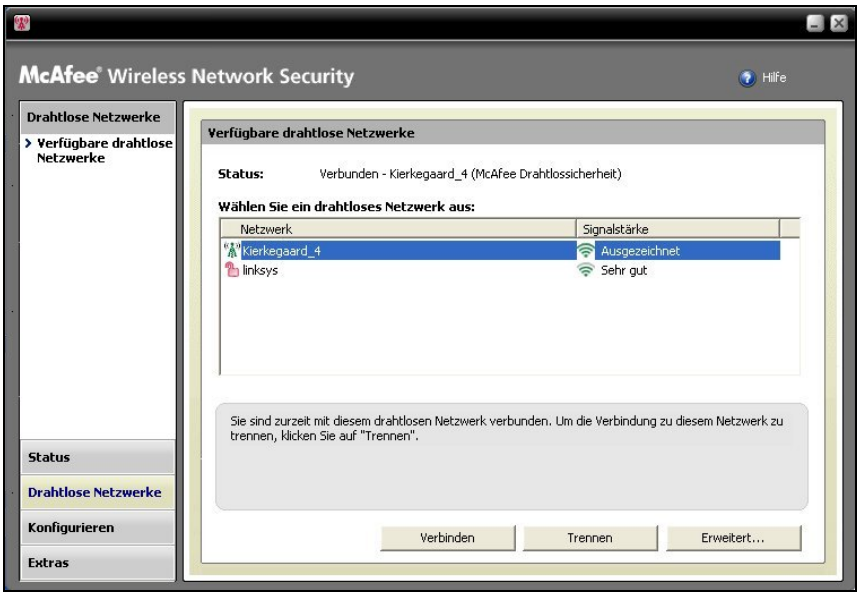
Gewähren von Netzwerkzugriff...
Verwaltetes Netzwerk - Kierkegaard_1
Aus Sicherheitsgründen...
Bestätigen Sie, dass die folgenden Karten von CORLOC-MWL-DE2 gesehen werden können, um das Gewähren des Zugriffs abzuschließen:
Hilfe
Zugriff gewähren
Zugriff verweigern

8 Der Bereich "Gewähren von Netzwerkzugriff" bestätigt, dass der neue Computer durch Wireless Network Security geschützt ist. Um die Sicherheitseinstellungen von anderen Computern zu überwachen und den anderen Computern zu erlauben, die Sicherheitseinstellungen Ihres Computers zu überwachen, wählen Sie **Es diesem und anderen Computern erlauben, gegenseitig ihre Sicherheitseinstellungen zu überwachen** aus.



9 Klicken Sie auf **Fertig**.

10 Der Bereich "Verfügbare drahtlose Netzwerke" zeigt an, dass Sie mit dem geschützten drahtlosen Netzwerk verbunden sind.



Verwandte Themen

- Computer zum geschützten drahtlosen Netzwerk hinzufügen (Seite 95)

Verbindung zu geschützten drahtlosen Netzwerken

Wenn Sie sich bereits an einem geschützten drahtlosen Netzwerk angemeldet und später die Verbindung abgebrochen haben und der Zugriff nicht widerrufen wurde, können Sie die Verbindung jederzeit wieder herstellen, ohne sich neu anmelden zu müssen.

So stellen Sie eine Verbindung zu einem geschützten drahtlosen Netzwerk her:

1 Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.

2 Wählen Sie **Drahtlose Netzwerke anzeigen** aus.

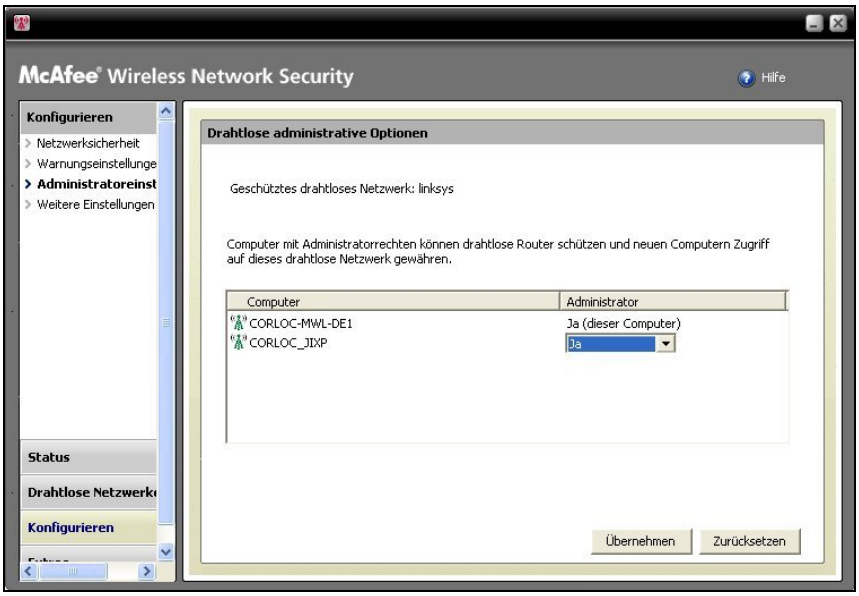
3 Wählen Sie im Bereich "Verfügbare drahtlose Netzwerke" ein Netzwerk aus, und klicken Sie auf **Verbinden**.

Computern administrativen Zugriff gewähren

Computer mit Administratorrechten können drahtlose Router schützen, Sicherheitsmodi ändern und neuen Computern Zugriff auf das geschützte drahtlose Netzwerk gewähren.

So konfigurieren Sie administrativen Zugriff:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Wählen Sie im Bereich "Konfigurieren" **Administratoreinstellungen** aus.
4. Wählen Sie im Bereich "Drahtlose Administratorrechte" **Ja** oder **Nein** aus, um administrativen Zugriff zu gewähren oder abzulehnen.



5. Klicken Sie auf **Übernehmen**.

Verwandte Themen

- Über Zugriffstypen (Seite 83)
- Netzwerkzugriffsrechte aufheben (Seite 111)

Schutz anderer drahtloser Geräte

Über Wireless Network Security können Sie andere drahtlose Geräte zum Netzwerk hinzufügen. Hierzu gehören: drahtlose Drucker, Druckserver oder Spielekonsolen.

So fügen Sie andere drahtlose Geräte hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Nicht-AP-Geräte schützen** auf **Schützen**.
4. Wählen Sie im Bereich "Drahtloses Gerät" ein drahtloses Gerät aus und klicken Sie auf **Schützen**.
5. Die Meldung "Gerät ohne Zugriffspunkt geschützt" bestätigt, dass das Gerät zum Netzwerk hinzugefügt wurde.

Verbindung zu Netzwerken mit deaktivierter SSID-Übertragung

Sie können eine Verbindung zu drahtlosen Netzwerken aufbauen, bei denen SSID-Übertragung deaktiviert ist. Router, bei denen SSID-Übertragung deaktiviert ist, erscheinen nicht im Bereich "Verfügbare drahtlose Netzwerke".

McAfee empfiehlt, dass Sie drahtlose Router, bei denen SSID-Übertragung deaktiviert ist, nicht mit Wireless Network Security schützen.

So stellen Sie eine Verbindung zu einem drahtlosen Netzwerk her, bei dem SSID-Übertragung deaktiviert ist:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Klicken Sie im Bereich "Verfügbare drahtlose Netzwerke" auf **Erweitert**.
4. Klicken Sie im Bereich "Drahtlose Netzwerke" auf **Hinzufügen**.
5. Legen Sie im Bereich "Drahtloses Netzwerk hinzufügen" die folgenden Einstellungen fest, und klicken Sie auf **OK**:

Einstellung	Beschreibung
Netzwerk	Der Name Ihres Netzwerks. Bei der Modifikation eines Netzwerks kann der Name nicht geändert werden.
Sicherheitseinstellungen	Die Sicherheit für Ihr ungeschütztes Netzwerk. Beachten Sie, dass, wenn der drahtlose Adapter den von Ihnen ausgewählten Modus nicht unterstützt, eine Verbindung nicht möglich ist. Zu den Sicherheitsmodi gehören: Deaktiviert, Open WEP, Shared WEP, Auto WEP, WPA-PSK, WPA2-PSK.
Verschlüsselungsmodus	Die zum ausgewählten Sicherheitsmodus gehörende Verschlüsselung. Zu den Verschlüsselungsmodi gehören: WEP, TKIP, AES und TKIP+AES.

Hinweis: McAfee empfiehlt, dass Sie drahtlose Router, bei denen SSID-Übertragung deaktiviert ist, nicht mit Wireless Network Security schützen. Wenn Sie diese Funktion verwenden müssen, tun Sie dies ausschließlich, wenn SSID-Übertragung deaktiviert ist.

Computer zum geschützten drahtlosen Netzwerk hinzufügen

Computer können zum geschützten drahtlosen Netzwerk mithilfe eines Wechselgeräts, wie beispielsweise USB-Flash-Laufwerk, beschreibbare CD oder die Windows Connect Now-Technologie, hinzugefügt werden.

Hinzufügen von Computern über Wechselgeräte

Über Wireless Network Security können Sie zusätzliche Computer, auf denen kein Wireless Network Security läuft, über ein USB-Flash-Laufwerk oder eine beschreibbare CD zum geschützten drahtlosen Netzwerk hinzufügen.

So fügen Sie einen Computer hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Computer schützen** auf **Schützen**.
4. Wählen Sie im Bereich "Anderen Computer schützen" **Kopieren Sie Wireless Network Security auf ein Wechselgerät, wie einen USB-Schlüssel** aus.

Anderen Computer schützen
Um einen anderen Computer zu schützen, auf dem Wireless Network Security ausgeführt wird, klicken Sie auf Hilfe.
Wenn der Computer nicht durch Wireless Network Security geschützt wird, führen Sie eine der folgenden Aktionen aus:
Kopieren Sie Wireless Network Security auf ein Wechselgerät, wie einen USB-Schlüssel.
Erstellen Sie eine Windows ConnectNow-Disk.
Speicherort auswählen:
USB MEMORY (H:)
Hilfe
Kopieren
Abbrechen

5 Wählen Sie den Ort des CD- oder des USB-Flash-Laufwerks, auf das Wireless Network Security kopiert werden soll.

6 Klicken Sie auf **Kopieren**.

7 Nachdem alle Dateien auf das CD- oder USB-Flash-Laufwerk kopiert wurden, legen Sie das Wechselgerät in den Computer ein, der geschützt werden soll. Sollte das Programm nicht automatisch starten, durchsuchen Sie den Inhalt des Wechselmediums über den Windows Explorer und klicken Sie auf **Install.exe**.

8 Befolgen Sie die Anweisungen auf dem Bildschirm.

Hinweis: Weiterhin können Sie mithilfe der Windows Connect Now-Technologie einen Computer zum geschützten drahtlosen Netzwerk hinzufügen.

Verwandte Themen

- Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie (Seite 97)

Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie

Über Wireless Network Security können Sie zusätzliche Computer, auf denen Wireless Network Security nicht ausgeführt wird, über die Windows Connect Now-Technologie hinzufügen.

So fügen Sie einen Computer mithilfe der Windows Connect Now-Technologie hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Computer schützen** auf **Schützen**.
4. Wählen Sie im Bereich "Anderen Computer schützen" **Windows Connect Now-Disk erstellen** aus.
5. Wählen Sie einen Speicherort für die Kopie der Windows Connect Now-Informationen.
6. Klicken Sie auf **Kopieren**.
7. Legen Sie die Windows Connect Now-Disk in den Computer ein, den Sie schützen möchten.
8. Führen Sie eine der folgenden Aktionen durch, wenn die Disk nicht automatisch starten sollte:
   - Installieren Sie die Wireless Connect Now-Technologie: Klicken Sie auf der Windows-Taskleiste auf **Start** und dann auf **Systemsteuerung**. Wenn Sie die Kategorieansicht der Systemsteuerung verwenden, klicken Sie auf **Netzwerk- und Internetverbindungen** und dann auf den **Assistent für die Einrichtung drahtloser Netzwerke**. Wenn Sie die klassische Ansicht der Systemsteuerung verwenden, klicken Sie auf **Assistent für die Einrichtung drahtloser Netzwerke**. Befolgen Sie die Anweisungen auf dem Bildschirm.
   - Öffnen Sie die Datei `setupSNK.exe` auf der Windows Connect-Disk, kopieren Sie den Schlüssel und fügen Sie diesen in den Auswahlclient Ihres drahtlosen Netzwerks ein.

Hinweis: Setzen Sie die Schlüsselrotation aus, wenn Sie die Windows Connect Now-Technologie für die Verbindung zum drahtlosen Netzwerk verwenden. Anderenfalls schlägt die Netzwerkverbindung fehl. Die Verbindung schlägt fehl, da die Schlüsselrotation einen neuen Schlüssel erstellt, der sich vom Schlüssel, den die Windows Connect Now-Technologie verwendet, unterscheidet.

Computer können zum geschützten drahtlosen Netzwerk weiterhin mithilfe eines Wechselgeräts, wie beispielsweise eine beschreibbare CD oder ein USB-Flash-Laufwerk, hinzugefügt werden.

Verwandte Themen

- Hinzufügen von Computern über Wechselgeräte (Seite 95)

KAPITEL 15

Drahtlosen Netzwerken verwalten

Wireless Network Security bietet einen vollständigen Satz an Administratortools für die Verwaltung und Pflege Ihres drahtlosen Netzwerks.

In diesem Kapitel

Verwalten drahtloser Netzwerke.....100

Verwalten drahtloser Netzwerke

Wenn Sie mit einem geschützten drahtlosen Netzwerk verbunden sind, werden die gesendeten und empfangenen Informationen verschlüsselt. Hacker können die im geschützten Netzwerk übertragenen Daten nicht entschlüsseln und auch keine Verbindung zu Ihrem Netzwerk herstellen. Wireless Network Security bietet eine Vielzahl von Tools, die Ihnen bei der Verwaltung Ihres Netzwerks behilflich sind, um weitere Intrusionen zu verhindern.

Über Wireless Network Security-Symbole

Wireless Network Security zeigt Symbole an, um diverse Netzwerkverbindungstypen und Signalstärken darzustellen.

Netzwerkverbindungssymbole

Die folgende Tabelle beschreibt die Symbole, die in Wireless Network Security in den Bereichen "Status des drahtlosen Netzwerks", "Sicherheitstools" und "Verfügbare drahtlose Netzwerke" zum Einsatz kommen. Die Symbole stellen diverse Netzwerkverbindungs- und Sicherheitsstatus dar.

Symbol	Statusbereiche	Schutzbereiche
	Ihr Computer ist mit dem ausgewählten geschützten drahtlosen Netzwerk verbunden.	Das Gerät ist durch Wireless Network Security geschützt.
	Ihr Computer kann auf das geschützte drahtlose Netzwerk zugreifen, aber ist derzeit nicht damit verbunden.	Das Gerät verwendet WEP- oder WPA-Sicherheit.
	Ihr Computer ist ein ehemaliges Mitglied des geschützten drahtlosen Netzwerks, aber das Zugriffsrecht wurde widerrufen, als die Verbindung des Computers mit dem Netzwerk aufgehoben wurde.	Für das Gerät ist Wireless Network Security deaktiviert.

Signalstärkensymbole

Die folgende Tabelle beschreibt die Symbole, die von Wireless Network Security für die Darstellung diverser Netzwerksignalstärken verwendet werden.

Symbol	Beschreibung
	Ausgezeichnete Signalstärke
	Sehr gute Signalstärke
	Gute Signalstärke
	Niedrige Signalstärke

Verwandte Themen

- Signalstärke des Netzwerks ansehen (Seite 134)
- Derzeit geschützte Computer ansehen (Seite 140)
- Netzwerksicherheitsmodus ansehen (Seite 132)

Bevorzugte Netzwerke auflisten

Über Wireless Network Security können Sie bevorzugte drahtlose Netzwerke festlegen. Hierüber können Sie die Reihenfolge der Netzwerke angeben, zu denen Ihr Computer automatisch eine Verbindung aufbaut. Wireless Network Security versucht zum ersten Netzwerk auf der Liste eine Verbindung aufzubauen.

Diese Funktion ist hilfreich, wenn Sie beispielsweise automatisch eine Verbindung zum drahtlosen Netzwerk eines Freundes aufbauen möchten, wenn Sie sich in der Nähe befinden. Sie können ein anderes Netzwerk auf den ersten Listenplatz setzen.

So listen Sie bevorzugte Netzwerke auf:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Klicken Sie im Bereich "Verfügbare drahtlose Netzwerke" auf **Erweitert**.
4. Wählen Sie das Netzwerk aus, dessen Listenplatz Sie anpassen möchten und klicken Sie auf **Nach oben** oder **Nach unten**.

5. Klicken Sie auf **OK**.

Verwandte Themen

- Bevorzugte drahtlose Netzwerke entfernen (Seite 103)

Bevorzugte drahtlose Netzwerke entfernen

Über Wireless Network Security können Sie bevorzugte Netzwerke entfernen.

Dies ist hilfreich, wenn Sie beispielsweise ein überflüssiges Netzwerk aus der Liste streichen möchten.

So entfernen Sie bevorzugte Netzwerke:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Klicken Sie im Bereich "Verfügbare drahtlose Netzwerke" auf **Erweitert**.
4. Wählen Sie im Bereich "Verfügbare drahtlose Netzwerke" ein Netzwerk aus, und klicken Sie auf **Entfernen**.
5. Klicken Sie auf **OK**.

Verwandte Themen

- Bevorzugte Netzwerke auflisten (Seite 102)

Geschützte drahtlose Netzwerke umbenennen

Über Wireless Network Security können Sie ein bestehendes geschütztes drahtloses Netzwerk umbenennen.

Das Umbenennen eines Netzwerks kann hilfreich sein, wenn beispielsweise Ihr Nachbar einen ähnlichen oder gleichen Namen verwendet, oder wenn Sie einen unverwechselbaren Namen erstellen möchten.

Computer, die mit dem geschützten drahtlosen Netzwerk verbunden sind, müssen möglicherweise eine manuelle Wiederherstellung der Verbindung durchführen und werden benachrichtigt, wenn sich der Name ändert.

Nach der Umbenennung des Netzwerks erscheint der Name im Bereich "Geschützter drahtloser Router/Zugriffspunkt".

So ändern Sie den Namen Ihres geschützten drahtlosen Netzwerks:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Geben Sie den neuen Namen im Bereich "Netzwerksicherheit" in das Feld **Name des geschützten drahtlosen Netzwerks** ein.
4. Klicken Sie auf **Übernehmen**.

   Das Dialogfenster "Netzwerk-Sicherheitseinstellungen werden aktualisiert" wird angezeigt, während Wireless Network Security den Namen des geschützten drahtlosen Netzwerks ändert. In Abhängigkeit von den Einstellungen Ihres Computers und der Signalstärke dauert die Namensänderung für das Netzwerk weniger als eine Minute.

Hinweis: Als Sicherheitsmaßnahme empfiehlt McAfee, dass Sie die Standard-SSID des Routers oder des Zugriffspunkts umbenennen. Obwohl Wireless Network Security Standard-SSIDs, wie beispielsweise "linksys" oder "belkin54g" oder "NETGEAR" unterstützt, schützt das Umbenennen der SSIDs vor Zugriffspunktbedrohungen.

Warneinstellungen konfigurieren

Über Wireless Network Security können Sie Warneinstellungen konfigurieren, um Warnungen anzeigen zu lassen, wenn bestimmte Ereignisse auftreten, wie beispielsweise der Verbindungsaufbau eines neuen Computers zum Netzwerk.

So konfigurieren Sie Warnverhalten:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Klicken Sie auf **Warneinstellungen**.
4. Wählen Sie eines oder mehrere der folgenden Ereignisse aus, oder entfernen Sie die Markierung, und klicken Sie auf **Übernehmen**:

Warnungseinstellung	Beschreibung
Der Sicherheitsschlüssel für Ihr geschütztes drahtloses Netzwerk wird rotiert.	Zeigt die Meldung "Sicherheitsschlüssel rotiert" an, nachdem der Sicherheitsschlüssel manuell oder automatisch rotiert wurde. Das Rotieren des Schlüssels schützt das Netzwerk vor Hackern, die versuchen, Ihre Daten abzufangen oder eine Verbindung zu Ihrem Netzwerk aufzubauen.
Ein anderer geschützter Computer stellt eine Verbindung zum Netzwerk her oder trennt eine Verbindung.	Zeigt die Meldungen "Computer verbunden" oder "Computer getrennt" an, nachdem ein Computer eine Verbindung zu einem geschützten drahtlosen Netzwerk aufgebaut oder getrennt hat. Die Daten auf verbundenen Computern sind jetzt gegen Intrusionen und Datenabfang geschützt.
Einem anderen Computer wird Zugriff auf Ihr geschütztes drahtloses Netzwerk gewährt.	Zeigt die Meldung "Computer hat Netzwerkzugriff gewährt" an, nachdem ein Administratorcomputer einem anderen Computer die Anmeldung zum geschützten drahtlosen Netzwerk gewährt hat. Einem Computer den Zugriff auf das geschützte Netzwerk zu gewähren, schützt vor Hackern, die versuchen, Ihre Daten abzufangen.
Die Schlüsselrotation für Ihr geschütztes drahtloses Netzwerk wird ausgesetzt oder wieder aufgenommen.	Zeigt entweder die Meldung "Schlüsselrotation ausgesetzt" oder "Schlüsselrotation fortgesetzt" an, nachdem Sie manuell die Schlüsselrotation ausgesetzt oder wieder aufgenommen haben. Das Rotieren des Schlüssels schützt das Netzwerk vor Hackern, die versuchen, Ihre Daten abzufangen oder eine Verbindung zu Ihrem Netzwerk aufzubauen.
Der Zugriff aller nicht verbundenen Computer wird widerrufen.	Zeigt die Meldung "Zugriff widerrufen" an, nachdem der Zugriff für Computer, die nicht mit dem Netzwerk verbunden sind, widerrufen wurde. Computer, deren Verbindung unterbrochen wurde, müssen sich erneut am Netzwerk anmelden.
Ein Router wurde zu Ihrem geschützten drahtlosen Netzwerk hinzugefügt oder daraus entfernt.	Zeigt die Meldungen "Router/Zugriffspunkt zum Netzwerk hinzugefügt" oder "Router/Zugriffspunkt ungeschützt" an, nachdem der Router oder der Zugriffspunkt zum geschützten drahtlosen Netzwerk hinzugefügt oder davon entfernt wurde.

Warnungseinstellung	Beschreibung
Die Anmeldeinformationen für einen geschützten drahtlosen Router wurden geändert.	Zeigt die Meldung "Anmeldeinformationen für Router/Zugriffspunkt geändert" an, nachdem der Wireless Network Security-Administrator den Benutzernamen oder das Kennwort eines Routers oder Zugriffspunkts geändert hat.
Der Name oder eine Sicherheitseinstellung Ihres geschützten drahtlosen Netzwerks wurde geändert.	Zeigt die Meldungen "Netzwerkeinstellungen geändert" oder "Netzwerk umbenannt" an, nachdem Sie das geschützte drahtlose Netzwerk umbenannt oder deren Sicherheitseinstellungen angepasst haben.
Die Einstellungen für Ihr geschütztes drahtloses Netzwerk werden repariert.	Zeigt die Meldung "Netzwerk repariert" an, nachdem Probleme in Bezug auf die Sicherheitseinstellungen auf den drahtlosen Routern oder Zugriffspunkten Ihres Netzwerks behoben wurden.

Hinweis: Um alle Warnmeldungen auszuwählen oder zu löschen, wählen Sie **Alles markieren** oder **Alles löschen**. Um die Warneinstellungen von Wireless Network Security zurückzusetzen, klicken Sie auf **Standardwerte wiederherstellen**.

Verwandte Themen

- Schlüssel automatisch rotieren (Seite 121)
- Anmelden an einem geschützten drahtlosen Netzwerk (Seite 86)
- Verbindung zu geschützten drahtlosen Netzwerken (Seite 91)
- Verbindung zum geschützten drahtlosen Netzwerk aufheben (Seite 110)
- Automatische Schlüsselrotation aussetzen (Seite 124)
- Netzwerkzugriffsrechte aufheben (Seite 111)
- Drahtlose Router oder Zugriffspunkte entfernen (Seite 109)
- Informationen für drahtlose Geräte ändern (Seite 117)
- Geschützte drahtlose Netzwerke umbenennen (Seite 104)
- Netzwerk-Sicherheitseinstellungen reparieren (Seite 118)

Verbindungsbenachrichtigung anzeigen

Sie können Wireless Network Security so einrichten, dass Sie eine Benachrichtigung erhalten, wenn Ihr Computer eine Verbindung mit einem drahtlosen Netzwerk aufbaut.

So lassen Sie die Benachrichtigung anzeigen, wenn eine Verbindung zu einem drahtlosen Netzwerk aufgebaut wird:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Wählen Sie **Bei einer Verbindung mit einem drahtlosen Netzwerk benachrichtigen** aus.
5. Klicken Sie auf **Übernehmen**.

Verwandte Themen

- Verbindung zu geschützten drahtlosen Netzwerken (Seite 91)

Drahtlose Router oder Zugriffspunkte entfernen

Über Wireless Network Security können Sie einen oder mehrere Router oder Zugriffspunkte von Ihrem geschützten Netzwerk entfernen.

So entfernen Sie einen drahtlosen Router oder Zugriffspunkt:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Den Schutz für ein Gerät aufheben** auf **Schutz aufheben**.
4. Wählen Sie im Bereich "Schutz für drahtlosen Router/Zugriffspunkt aufheben" einen drahtlosen Router oder Zugriffspunkt aus, der vom geschützten Netzwerk entfernt werden soll, und klicken Sie auf **Schutz aufheben**.

Schutz für drahtlosen Router/Zugriffspunkt aufheben
Wählen Sie einen drahtlosen Router oder Zugriffspunkt aus, der aus Ihrem geschützten Netzwerk entfernt werden soll.
Drahtloser Router oder Zugriffspunkt
Netzwerk
Linksys WRT54G (192.168.1.1)
Kierkegaard_1
Aktualisieren
Dieser drahtlose Router oder Zugriffspunkt ist derzeit geschützt. Klicken Sie zum Aufheben des Schutzes auf "Schutz aufheben".
Schutz aufheben
Abbrechen
Hilfe

5. Klicken Sie im Dialogfeld "Drahtloser Router/Zugriffspunkt ungeschützt" auf **OK**, um zu bestätigen, dass der Router oder der Zugriffspunkt vom Netzwerk entfernt wurde.

Verwandte Themen

- Geschützte drahtlose Netzwerke erstellen (Seite 84)

Verbindung zum geschützten drahtlosen Netzwerk aufheben

Über Wireless Network Security können Sie die Verbindung Ihres Computers zum Netzwerk aufheben.

Diese Funktion ist hilfreich, wenn Ihr Computer beispielsweise eine Verbindung zu einem Netzwerk unter Verwendung eines Namens aufgebaut hat, der mit dem Netzwerknamen übereinstimmt. Sie können die Verbindung zum Netzwerk aufheben und dann eine erneute Verbindung zu Ihrem Netzwerk herstellen.

Diese Funktion ist hilfreich, wenn Sie aus Versehen aufgrund einer hohen Signalstärke eines anderen Zugriffspunkts oder einer Funktionsstörung eine Verbindung zu einem falschen Netzwerk aufgebaut haben.

So heben Sie eine Verbindung zu einem geschützten drahtlosen Netzwerk auf:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Wählen Sie im Bereich "Verfügbare drahtlose Netzwerke" ein Netzwerk aus und klicken Sie auf **Trennen**.

Verwandte Themen

- Netzwerkzugriffsrechte aufheben (Seite 111)
- Geschützte drahtlose Netzwerke verlassen (Seite 112)

Netzwerkzugriffsrechte aufheben

Über Wireless Network Security können Sie den Zugriff von Computern ablehnen, die nicht mit dem Netzwerk verbunden sind. Es wird ein neuer Rotationsplan für den Sicherheitsschlüssel aufgestellt: Computer, die nicht verbunden sind, verlieren den Zugriff auf das geschützte drahtlose Netzwerk, aber können den Zugriff wieder erlangen, wenn Sie sich erneut am Netzwerk anmelden. Der Zugriff verbundener Computer wird aufrechterhalten.

Beispielsweise können Sie den Zugriff eines Besuchercomputer mit Wireless Network Security widerrufen, nachdem diese die Verbindung getrennt hat. Zusätzlich kann ein Erwachsener aus Jugendschutzgründen den Zugriff eines Computers, der von einem Kind verwendet wird, widerrufen. Ein zuvor versehentlich gewährter Zugriff kann ebenfalls widerrufen werden.

So widerrufen Sie den Zugriff aller Computer, deren Verbindung zum geschützten Netzwerk getrennt ist:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Extras" auf "Wartungstools".
4. Klicken Sie im Bereich "Wartungstools" unter **Zugriff widerrufen** auf **Widerrufen**.
5. Klicken Sie im Bereich "Zugriff widerrufen" auf **Widerrufen**.
6. Klicken Sie im Wireless Network Security-Dialogfeld auf **OK**.

Verwandte Themen

- Verbindung zum geschützten drahtlosen Netzwerk aufheben (Seite 110)
- Geschützte drahtlose Netzwerke verlassen (Seite 112)

Geschützte drahtlose Netzwerke verlassen

Sie können Wireless Network Security dazu verwenden, Ihre Zugriffrechte auf ein geschütztes Netzwerk abzubrechen.

So verlassen Sie ein Netzwerk:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Wählen Sie im Bereich "Konfigurieren" **Weitere Einstellungen** aus.
4. Wählen Sie im Bereich "Weitere Einstellungen" unter "Zugriff auf geschütztes Netzwerk" das Netzwerk aus, das Sie verlassen möchten und klicken Sie auf **Netzwerk verlassen**.
5. Klicken Sie im Bereich "Verbindung zum Netzwerk trennen" auf **Ja**, um das Netzwerk zu verlassen.

Hinweis: Wenn Sie ein Netzwerk verlassen haben, muss Ihnen ein anderer Benutzer den Zugriff auf das geschützte Netzwerk wieder gewähren, bevor Sie sich erneut an diesem Netzwerk anmelden können.

Verwandte Themen

- Verbindung zum geschützten drahtlosen Netzwerk aufheben (Seite 110)
- Netzwerkzugriffsrechte aufheben (Seite 111)

KAPITEL 16

Sicherheit für drahtloses Netzwerk verwalten

Wireless Network Security bietet einen vollständigen Satz an Tools für die Verwaltung der Sicherheitsfunktionen Ihres drahtlosen Netzwerks.

In diesem Kapitel

Konfigurieren von Sicherheitseinstellungen.....114
Netzwerkschlüssel verwalten 119

Konfigurieren von Sicherheitseinstellungen

Nachdem Sie eine Verbindung zu einem geschützten drahtlosen Netzwerk aufgebaut haben, schützt Wireless Network Security automatisch Ihr Netzwerk. Allerdings können Sie jederzeit zusätzliche Sicherheitseinstellungen konfigurieren.

Sicherheitsmodi konfigurieren

Sie können den Sicherheitsmodus Ihres geschützten drahtlosen Netzwerks festlegen. Sicherheitsmodi definieren die Verschlüsselung zwischen Ihrem Computer und dem Router oder Zugriffspunkt.

Wenn Sie Ihr Netzwerk schützen, wird WEP automatisch konfiguriert. Allerdings empfiehlt McAfee, dass Sie den Sicherheitsmodus auf WPA2 oder WPA-PSK AES ändern. Wireless Network Security verwendet anfänglich WEP, da dieser Modus von allen Routern und Adaptern für drahtlose Netzwerke unterstützt wird. Die meisten neuen Router und Adapter für drahtlose Netzwerke arbeiten allerdings im WPA-Modus. Dieser ist sicherer.

So ändern Sie den Sicherheitsmodus für ein geschütztes drahtloses Netzwerk:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Wählen Sie im Bereich "Netzwerksicherheit" im Feld **Sicherheitsmodus** die Sicherheitsmethode aus, die Sie verwenden möchten und klicken Sie auf **Übernehmen**.

Die folgende Tabelle beschreibt die verfügbaren Sicherheitsmodi:

Stärke	Modus	Beschreibung
Schwächste	WEP	Wired Equivalent Privacy (WEP) ist Teil der Norm IEEE 802.11 für drahtlose Netzwerke zur Sicherung von drahtlosen IEEE 802.11-Netzwerken. WEP bietet eine Sicherheitsstufe, die einen schwachen Versuch, in die Privatsphäre einzudringen, verhindern kann, aber nicht so sicher ist wie die WPA-PSK-Verschlüsselung. Obwohl Wireless Network Security einen starken (schwer zu erratenden und langen) Schlüssel erstellt, empfiehlt McAfee, dass Sie einen WPA-Sicherheitsmodus verwenden.
Durchschnittlich	WPA-PSK TKIP	Wi-Fi Protected Access (WPA) ist eine frühe Version des Sicherheitsstandards 802.11i. TKIP wurde für WPA entwickelt, um WEP zu verbessern. TKIP bietet Nachrichtenintegrität, Mechanismen zur Neuverteilung von Schlüsseln und Paketschlüsselmischung.
Stark	WPA-PSK AES	Dieser Sicherheitsmodus kombiniert WPA- und AES-Modi. Advanced Encryption Standard (AES) ist eine Blockchiffre, die von der US-Regierung als Verschlüsselungsstandard verwendet wird.
Stärkere	WPA2-PSK AES	Dieser Sicherheitsmodus kombiniert WPA2- und AES-Modi. WPA2 ist die nächste Erweiterung der Ratifizierung des Sicherheitsstandards 802.11i. WPA2 bindet Counter Mode CBC MAC Protocol (CCMP) ein. Diese Lösung ist sicherer und skalierbarer als TKIP. Hierbei handelt es sich um den stärksten Sicherheitsmodus, der Verbrauchern zur Verfügung steht.

Stärke	Modus	Beschreibung
Stärkste	WPA2-PSK TKIP+AES	Dieser Sicherheitsmodus kombiniert WPA2- und AES- als auch WPA-PSK TKIP-Modi. Hierbei ist eine größere Flexibilität möglich, so dass sowohl alte als auch neue drahtlose Adapter angeschlossen werden können.

Hinweis: Nach der Änderung des Sicherheitsmodus ist es möglicherweise notwendig, dass Sie erneut manuell eine Verbindung aufbauen.

Verwandte Themen

- Netzwerk-Sicherheitseinstellungen reparieren (Seite 118)
- Netzwerksicherheitsmodus ansehen (Seite 132)

Netzwerk-Sicherheitseinstellungen konfigurieren

Sie können die Netzwerkeinstellungen von Netzwerken, die durch Wireless Network Security geschützt sind, ändern. Dies ist beispielsweise hilfreich, wenn Sie die Sicherheit von WEP auf WPA aufrüsten möchten.

McAfee empfiehlt, dass Sie die Netzwerk-Sicherheitseinstellungen ändern, wenn Sie durch eine Meldung dazu aufgefordert werden.

So konfigurieren Sie die Eigenschaften eines ungeschützten Netzwerks:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Klicken Sie im Bereich "Verfügbare drahtlose Netzwerke" auf **Erweitert**.
4. Klicken Sie im Bereich "Drahtlose Netzwerke" auf **Eigenschaften**.
5. Ändern Sie im Bereich "Eigenschaften des drahtlosen Netzwerks" die folgenden Einstellungen, und klicken Sie auf **OK**:

Einstellung	Beschreibung
Netzwerk	Der Name Ihres Netzwerks. Bei der Modifikation eines Netzwerks kann der Name nicht geändert werden.

Einstellung	Beschreibung
Sicherheitseinstellungen	Die Sicherheit für Ihr ungeschütztes Netzwerk. Beachten Sie, dass wenn der drahtlose Adapter den von Ihnen ausgewählten Modus nicht unterstützt, eine Verbindung nicht möglich ist. Zu den Sicherheitsmodi gehören: Deaktiviert, Open WEP, Shared WEP, Auto WEP, WPA-PSK, WPA2-PSK.
Verschlüsselungsmodus	Die zum ausgewählten Sicherheitsmodus gehörende Verschlüsselung. Zu den Verschlüsselungsmodi gehören: WEP, TKIP, AES und TKIP+AES.

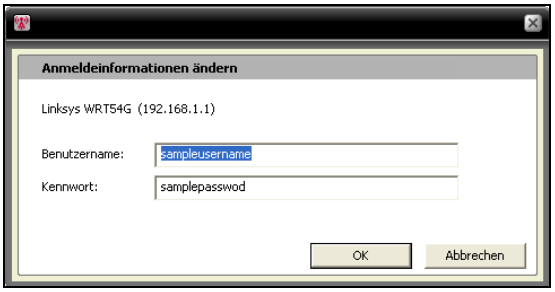
Informationen für drahtlose Geräte ändern

Sie können den Benutzernamen und das Kennwort für ein Gerät auf Ihrem geschützten drahtlosen Router oder Zugriffspunkt ändern. Die Liste der Geräte erscheint unter **Geschützte drahtlose Netzwerkgeräte**.

McAfee empfiehlt, dass Sie Ihre Anmeldeinformationen ändern, da die Mehrzahl der drahtlosen Geräte, die von einem Hersteller sind, dieselben Anmeldeinformationen aufweisen. Das Ändern der Anmeldeinformationen hilft zu verhindern, dass andere auf Ihren drahtlosen Router oder Zugriffspunkt zugreifen und Einstellungen ändern können.

So ändern Sie den Benutzernamen oder das Kennwort für ein geschütztes drahtloses Netzwerkgerät:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Wählen Sie im Bereich "Netzwerksicherheit" unter **Geschützte drahtlose Netzwerkgeräte** einen drahtlosen Router oder Zugriffspunkt aus, und klicken Sie auf **Benutzernamen oder Kennwort ändern**.



4 Klicken Sie nach der Eingabe der Anmeldeinformationen im Dialogfenster "Wireless Network Security" auf **OK**.

Der neue Benutzername und das neue Kennwort erscheinen unter **Geschützte drahtlose Netzwerkgeräte**.

Hinweis: Einige Router unterstützen die Verwendung von Benutzernamen nicht. Daher erscheint kein Benutzername unter **Geschützte drahtlose Netzwerkgeräte**.

Netzwerk-Sicherheitseinstellungen reparieren

Wenn Sie Schwierigkeiten mit den Sicherheitseinstellungen oder der Konfiguration haben sollten, können Sie über Wireless Network Security die Einstellungen für Ihren Router oder Zugriffspunkt reparieren.

So reparieren Sie Ihre Sicherheitseinstellungen:

1 Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.

2 Wählen Sie **Tools anzeigen** aus.

3 Klicken Sie im Bereich "Extras" auf **Wartungstools**.

4 Klicken Sie unter **Netzwerk-Sicherheitseinstellungen reparieren** auf **Reparieren**.

5 Klicken Sie im Bereich "Netzwerk-Sicherheitseinstellungen reparieren" auf **Reparieren**.

Eine Wireless Network Security-Meldung zeigt an, ob das Netzwerk repariert werden konnte oder nicht.

Hinweis: Sollte der Versuch, das Netzwerk zu reparieren, fehlschlagen, stellen Sie eine Verbindung zum Netzwerk über Kabel her, und versuchen Sie es erneut. Sollte sich das Kennwort für Router oder Zugriffspunkt geändert haben, müssen Sie das Kennwort neu eingeben, um eine Verbindung aufzubauen.

Netzwerkschlüssel verwalten

Wireless Network Security erstellt mithilfe eines Zufallsgenerators lange, starke und zufällige Verschlüsselungsschlüssel. Bei WEP wird der Schlüssel in einen hexadezimalen Wert mit 26 Zeichen übersetzt (für 104 Bits mittlerem Informationsgehalt oder Stärke, maximal durch 128-Bit-WEP unterstützte Stärke), während bei WPA der Schlüssel eine ASCII-Zeichenkette mit 63 Zeichen ist. Jedes Zeichen hat 64 mögliche Werte (6 Bits), wobei 384 Bits für den mittleren Informationsgehalt aufgebracht werden. Dies überschreitet die WAP-Schlüsselstärke von 256 Bits.

Bei der Verwaltung von Netzwerkschlüsseln können die Schlüssel als Klartext oder als Sternchen (für nicht geschützte Zugriffspunkte) angezeigt, gespeicherte Schlüssel für nicht geschützte Zugriffspunkte verworfen, Schlüsselrotation aktiviert oder deaktiviert, die Schlüsselrotationshäufigkeit geändert und die Schlüsselrotation ausgesetzt werden.

Bei einer automatischen Schlüsselrotation können die Tools der Hacker Ihre Daten nicht abfangen, da sich der Schlüssel fortwährend ändert.

Wenn Sie drahtlose Geräte, die von Wireless Network Security nicht unterstützt werden, mit dem Netzwerk verbinden (z. B. einen Handheld), müssen Sie den Schlüssel notieren, die Schlüsselrotation anhalten und den Schlüssel in das Gerät eingeben.

Aktuelle Schlüssel anzeigen

Wireless Network Security bietet einen schnellen Zugriff auf die drahtlosen Sicherheitsinformationen, einschließlich dem aktuellen Schlüssel für ein geschütztes drahtloses Netzwerk.

So lassen Sie den aktuellen Schlüssel anzeigen:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.
3. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" unter "Geschütztes drahtloses Netzwerk" auf **Aktueller Schlüssel**.

   Der für Ihr Netzwerk konfigurierte Schlüssel erscheint im Dialogfenster "Schlüsselkonfiguration".

Verwandte Themen

- Anzahl der Schlüsselrotationen einsehen (Seite 137)

Schlüssel automatisch rotieren

Standardmäßig ist die automatische Schlüsselrotation aktiviert. Wenn Sie allerdings die Schlüsselrotation aussetzen, kann diese über einen Computer mit Administratorrechten wieder aktiviert werden.

Sie können Wireless Network Security so konfigurieren, dass der Sicherheitsschlüssel eines geschützten drahtlosen Netzwerks automatisch rotiert wird.

Wireless Network Security erstellt automatisch eine unbegrenzte Serie an starken Schlüsseln, die über das Netzwerk synchronisiert wird. Die drahtlose Verbindung kann kurz unterbrochen werden, während der drahtlose Router mit der neuen Konfiguration des Sicherheitsschlüssels neu gestartet wird. Dies geschieht üblicherweise von den Netzwerkbenutzern unbemerkt.

Sollte kein Computer mit dem Netzwerk verbunden sein, tritt die Schlüsselrotation mit dem Verbindungsaufbau des ersten Computers auf.

So aktivieren Sie die automatische Schlüsselrotation:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Markieren Sie im Bereich "Netzwerksicherheit" die Option **Automatische Schlüsselrotation aktivieren.**

   Die Schlüsselrotation kann auch vom Bereich "Status des drahtlosen Netzwerks" wieder aufgenommen werden.
4. Klicken Sie auf **Übernehmen**.

Hinweis: Die Schlüsselrotation geschieht standardmäßig alle drei Stunden. Sie können die Häufigkeit der Schlüsselrotation allerdings auf Ihre Anforderungen anpassen.

Verwandte Themen

- Schlüsselrotationshäufigkeit anpassen (Seite 122)
- Schlüsselrotation fortsetzen (Seite 122)
- Anzahl der Schlüsselrotationen einsehen (Seite 137)

Schlüsselrotation fortsetzen

Obwohl die automatische Schlüsselrotation standardmäßig aktiviert ist, kann ein Computer mit Administratorrechten die Schlüsselrotation nach einer Aussetzung wieder aufnehmen.

So nehmen Sie die Schlüsselrotation wieder auf:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen** aus.
3. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" auf **Schlüsselrotation fortsetzen**.

   Die Meldungen "Schlüsselrotation gestartet" und "Sicherheitsschlüssel rotiert" bestätigen den Start der Schlüsselrotation und die erfolgreiche Durchführung.

Verwandte Themen

- Schlüssel automatisch rotieren (Seite 121)
- Automatische Schlüsselrotation aussetzen (Seite 124)
- Anzahl der Schlüsselrotationen einsehen (Seite 137)

Schlüsselrotationshäufigkeit anpassen

Wenn Wireless Network Security für die automatische Rotation des Sicherheitsschlüssels des drahtlosen Netzwerks konfiguriert ist, können Sie den Zeitraum anpassen, nach dem diese Schlüsselrotation stattfindet. Dieser Zeitraum kann von 15 Minuten bis 15 Tagen reichen.

McAfee empfiehlt eine tägliche Rotation des Sicherheitsschlüssels.

So passen Sie die automatische Schlüsselrotationshäufigkeit an:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Bestätigen Sie im Bereich "Netzwerksicherheit", dass die automatische Schlüsselrotation aktiviert ist, und bewegen Sie den Schieberegler für die **Häufigkeit** auf eine der folgenden Positionen:
   - **alle 15 Minuten**
   - **alle 30 Minuten**
   - **jede Stunde**
   - **alle 3 Stunden**

- **alle 12 Stunden**
- **jeden Tag**
- **alle 7 Tage**
- **alle 15 Tage**

4 Klicken Sie auf **Übernehmen**.

Hinweis: Stellen Sie sicher, dass die automatische Schlüsselrotation aktiviert ist, bevor Sie die Schlüsselrotationshäufigkeit einstellen.

Verwandte Themen

- Automatische Schlüsselrotation aktivieren (Seite 121)
- Anzahl der Schlüsselrotationen einsehen (Seite 137)

Automatische Schlüsselrotation aussetzen

Die Schlüsselrotation kann von jedem Computer, der mit dem drahtlosen Netzwerk verbunden ist, ausgesetzt werden. Möglicherweise möchten Sie die Schlüsselrotation aussetzen, um Folgendes durchzuführen:

- Sie möchten einem Gast, der nicht über Wireless Network Security verfügt, den Zugriff zum Netzwerk gewähren.
- Sie möchten einem Nicht-Windows-System, z. B. Macintosh, Linux oder TiVo, Zugriff gewähren. Nachdem Sie die Schlüsselrotation angehalten haben, notieren Sie den Schlüssel, und geben Sie ihn in das neue Gerät ein.
- Sie möchten eine drahtlose Verbindung ermöglichen, die nicht durch Schlüsselrotationen unterbrochen wird, um bestimmte Programme, wie z. B. Online-Spiele, durchzuführen.
- Sie sollten die Schlüsselrotation möglichst bald fortsetzen, damit das Netzwerk vor Hackern vollständig geschützt ist.

So lassen Sie den aktuellen Schlüssel anzeigen:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen** aus.
3. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" unter "Geschütztes drahtloses Netzwerk" auf **Aktueller Schlüssel**. Notieren Sie den Schlüssel, der im Dialogfenster "Schlüsselkonfiguration" angegeben ist. Andere Computer, auf denen kein Wireless Network Security installiert ist, können über diesen Schlüssel eine Verbindung zum geschützten drahtlosen Netzwerk aufbauen.
4. Klicken Sie im Dialogfenster "Schlüsselkonfiguration" auf **Schlüsselrotation aussetzen**.
5. Klicken Sie im Dialogfenster "Schlüsselrotation ausgesetzt" auf **OK**, um mit der Arbeit fortzufahren.

Warnung: Wird die Schlüsselrotation nicht ausgesetzt, verlieren die nicht unterstützten drahtlosen Geräte, die manuell mit dem Netzwerk verbunden sind, die Verbindung, wenn der Schlüssel rotiert.

Sie können eine Windows Connect Now-Disk erstellen und dann über die Textdatei den Schlüssel auf den anderen Computer oder das andere Gerät kopieren.

Verwandte Themen

- Automatische Schlüsselrotation aktivieren (Seite 121)

- Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie (Seite 97)
- Schlüsselrotation fortsetzen (Seite 122)
- Schlüssel automatisch rotieren (Seite 121)
- Anzahl der Schlüsselrotationen einsehen (Seite 137)

Netzwerkschlüssel manuell rotieren

Über Wireless Network Security können Sie einen Netzwerkschlüssel manuell rotieren, auch wenn die automatische Schlüsselrotation aktiviert ist.

So rotieren Sie einen Netzwerkschlüssel manuell:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Extras" auf **Wartungstools**.
4. Klicken Sie auf der Seite "Wartungstools" unter **Sicherheitsschlüssel manuell rotieren** auf **Rotieren**.

   Die Meldung "Schlüsselrotation gestartet" erscheint und bestätigt, dass die Schlüsselrotation begonnen hat. Nach der Rotation des Sicherheitsschlüssels bestätigt die Meldung "Sicherheitsschlüssel rotiert", dass der Sicherheitsschlüssel erfolgreich rotiert wurde.

Hinweis: Um die Verwaltung der Sicherheitsschlüssel zu vereinfachen, können Sie im Bereich "Netzwerksicherheit" die automatische Schlüsselrotation aktivieren.

Sollte kein Computer mit Ihrem drahtlosen Netzwerk verbunden sein, tritt die automatische Schlüsselrotation mit dem Verbindungsaufbau des ersten Computers auf.

Verwandte Themen

- Automatische Schlüsselrotation aktivieren (Seite 121)
- Schlüsselrotationshäufigkeit anpassen (Seite 122)
- Anzahl der Schlüsselrotationen einsehen (Seite 137)

Schlüssel als Sternchen darstellen

Schlüssel werden standardmäßig als Sternchen dargestellt. Sie können Wireless Network Security allerdings auch so einrichten, dass die Schlüssel auf Netzwerken, die nicht durch Wireless Network Security geschützt sind, im Textformat angezeigt werden.

Netzwerke, die durch Wireless Network Security geschützt sind, zeigen die Schlüssel im Textformat an.

So lassen Sie Schlüssel als Sternchen darstellen:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen**.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Entfernen Sie die Markierung für das Kontrollkästchen **Schlüssel in Klartext anzeigen**.
5. Klicken Sie auf **Übernehmen**.

Verwandte Themen

- Schlüssel in Klartext anzeigen (Seite 127)

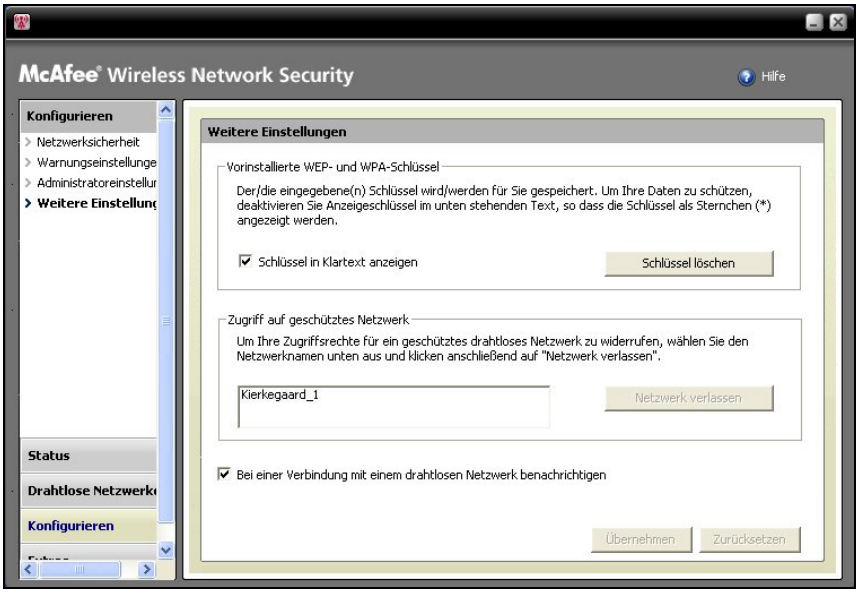
Schlüssel in Klartext anzeigen

Schlüssel werden standardmäßig als Sternchen dargestellt. Sie können Wireless Network Security allerdings auch so einrichten, dass die Schlüssel auf Netzwerken, die nicht durch Wireless Network Security geschützt sind, im Textformat angezeigt werden.

Netzwerke, die durch Wireless Network Security geschützt sind, zeigen die Schlüssel im Textformat an.

So lassen Sie Schlüssel in Klartext darstellen:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen**.
3. Klicken Sie auf **Weitere Einstellungen**.


McAfee® Wireless Network Security
Hilfe
Konfigurieren
Netzwerksicherheit
Warnungseinstellunge
Administratoreinstellur
Weitere Einstellung
Status
Drahtlose Netzwerke
Konfigurieren
Weitere Einstellungen
Vorinstallierte WEP- und WPA-Schlüssel
Der/die eingegebene(n) Schlüssel wird/werden für Sie gespeichert. Um Ihre Daten zu schützen, deaktivieren Sie Anzeigeschlüssel im unten stehenden Text, so dass die Schlüssel als Sternchen (*) angezeigt werden.
Schlüssel in Klartext anzeigen
Schlüssel löschen
Zugriff auf geschütztes Netzwerk
Um Ihre Zugriffsrechte für ein geschütztes drahtloses Netzwerk zu widerrufen, wählen Sie den Netzwerknamen unten aus und klicken anschließend auf "Netzwerk verlassen".
Kierkegaard_1
Netzwerk verlassen
Bei einer Verbindung mit einem drahtlosen Netzwerk benachrichtigen
Übernehmen
Zurücksetzen

4. Markieren Sie das Kontrollkästchen **Schlüssel in Klartext anzeigen**.
5. Klicken Sie auf **Übernehmen**.

Verwandte Themen

- Schlüssel als Sternchen darstellen (Seite 126)

Netzwerkschlüssel löschen

Wireless Network Security speichert automatisch Ihre WEP- und vorinstallierten WPA-Schlüssel. Diese können Sie jederzeit löschen.

So löschen Sie alle Netzwerkschlüssel:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen**.
3. Klicken Sie im Bereich **Konfigurieren** auf **Weitere Einstellungen**.
4. Klicken Sie im Bereich **Weitere Einstellungen** unter **Vorinstallierte WEP- und WPA-Schlüssel** auf **Schlüssel löschen**.
5. Klicken Sie im Dialogfeld "Schlüssel löschen" auf **Ja**, wenn Sie sicher sind, dass Sie alle gespeicherten, vorinstallierten WEP- und WPA-Schlüssel löschen möchten.

Warnung: Durch das Löschen der Schlüssel werden diese permanent von Ihrem Computer entfernt. Nach dem Löschen der Netzwerkschlüssel müssen Sie den richtigen Schlüssel eingeben, um eine Verbindung zu einem WEP- und WPA-Netzwerk aufzubauen.

KAPITEL 17

Drahtlose Netzwerke überwachen

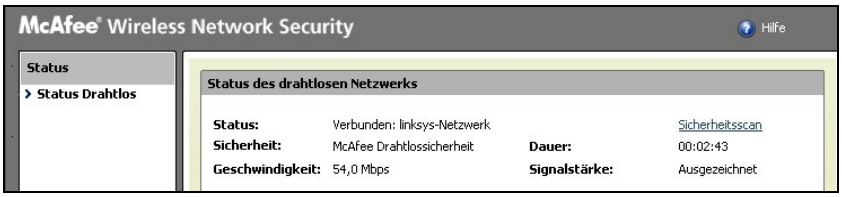
Über Wireless Network Security können Sie den Status Ihres drahtlosen Netzwerks und geschützten Computer überwachen.

In diesem Kapitel

Drahtlose Netzwerkverbindungen überwachen.....130
Geschützte drahtlose Netzwerke überwachen 136
Problembehandlung.....141

Drahtlose Netzwerkverbindungen überwachen

Im Bereich "Status des drahtlosen Netzwerks" können Sie den Status Ihrer Netzwerkverbindung, Sicherheitsmodus, Geschwindigkeit, Dauer, Signalstärke und Sicherheitsbericht ansehen.



Die folgende Tabelle beschreibt die Statusindikatoren für drahtlose Netzwerkverbindungen.

Status	Beschreibung	Informationen
Status	Zeigt an, ob Ihr Computer mit einem Netzwerk verbunden ist, und wenn ja, mit welchem.	Verbindungsstatus ansehen (Seite 131)
Sicherheit	Zeigt den Sicherheitsmodus des Netzwerks an, mit dem Sie verbunden sind. Wireless Network Security wird angezeigt, wenn Sie durch Wireless Network Security geschützt sind.	Netzwerksicherheitsmodus ansehen (Seite 133)
Geschwindigkeit	Zeigt die Geschwindigkeit der Verbindung Ihres Computers zum Netzwerk an.	Netzwerkverbindungsgeschwindigkeit ansehen (Seite 133)
Dauer	Zeigt die Zeit an, die Ihr Computer mit dem Netzwerk verbunden ist.	Dauer der Netzwerkverbindung ansehen (Seite 133)
Signalstärke	Zeigt die relative Signalstärke des Netzwerks an.	Signalstärke des Netzwerks ansehen (Seite 134)

Status	Beschreibung	Informationen
Sicherheits-scan	Durch Klicken auf **Sicherheitsscan** werden Sicherheitsinformationen, z. B. Sicherheitslücken im drahtlosen Netzwerk, Leistungsprobleme und der Status des drahtlosen Netzwerks angezeigt.	Online-Sicherheitsbericht ansehen (Seite 134)

Verwandte Themen

- Über Wireless Network Security-Symbole (Seite 100)

Verbindungsstatus ansehen

Über den Bereich "Status des drahtlosen Netzwerks" können Sie den Status der Netzwerkverbindung prüfen, um zu bestätigen, ob Sie mit dem Netzwerk verbunden sind oder nicht.

So sehen Sie den Status der drahtlosen Verbindung ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Die Computer, die mit dem geschützten Netzwerk verbunden sind, als auch Zeit und Datum der Verbindungen werden im Bereich "Status des drahtlosen Netzwerks unter **Computer** angezeigt.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 130)
- Netzwerksicherheitsmodus ansehen (Seite 133)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 133)
- Dauer der Netzwerkverbindung ansehen (Seite 133)
- Signalstärke des Netzwerks ansehen (Seite 134)
- Online-Sicherheitsbericht ansehen (Seite 134)

Netzwerksicherheitsmodus ansehen

Über den Bereich "Status der drahtlosen Verbindung" können Sie den Sicherheitsmodus der Netwerkverbindung prüfen.

So sehen Sie den Netzwerksicherheitsmodus ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Der Sicherheitsmodus wird im Bereich "Status des drahtlosen Netzwerks" im Feld **Sicherheit** angezeigt.

   Wireless Network Security wird angezeigt, wenn das drahtlose Netzwerk durch Wireless Network Security geschützt ist.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 130)
- Verbindungsstatus ansehen (Seite 131)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 133)
- Dauer der Netzwerkverbindung ansehen (Seite 133)
- Signalstärke des Netzwerks ansehen (Seite 134)
- Online-Sicherheitsbericht ansehen (Seite 134)

Netzwerkverbindungsgeschwindigkeit ansehen

Über den Bereich "Status des drahtlosen Netzwerks" können Sie die Geschwindigkeit der Verbindung Ihres Computers zum Netzwerk prüfen.

So sehen Sie die Netzwerkverbindungsgeschwindigkeit ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Die Verbindungsgeschwindigkeit wird im Bereich "Status des drahtlosen Netzwerks" im Feld **Geschwindigkeit** angezeigt.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 130)
- Verbindungsstatus ansehen (Seite 131)
- Netzwerksicherheitsmodus ansehen (Seite 133)
- Dauer der Netzwerkverbindung ansehen (Seite 133)
- Signalstärke des Netzwerks ansehen (Seite 134)
- Online-Sicherheitsbericht ansehen (Seite 134)

Dauer der Netzwerkverbindung ansehen

Über den Bereich "Status des drahtlosen Netzwerks" können Sie die Dauer der Verbindung zum Netzwerk prüfen.

So sehen Sie die Dauer der Verbindung zum Netzwerk ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Die Zeitdauer, in der Ihr Computer mit dem drahtlosen Netzwerk verbunden war, wird im Feld **Dauer** angezeigt.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 130)
- Verbindungsstatus ansehen (Seite 131)
- Netzwerksicherheitsmodus ansehen (Seite 133)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 133)
- Signalstärke des Netzwerks ansehen (Seite 134)
- Online-Sicherheitsbericht ansehen (Seite 134)

Signalstärke des Netzwerks ansehen

Über den Bereich "Status der drahtlosen Verbindung" können Sie die Signalstärke des Netzwerks prüfen.

So sehen Sie die Signalstärke ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Die Qualität des Signals wird im Feld **Signalstärke** angezeigt.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 130)
- Verbindungsstatus ansehen (Seite 131)
- Netzwerksicherheitsmodus ansehen (Seite 133)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 133)
- Dauer der Netzwerkverbindung ansehen (Seite 133)
- Online-Sicherheitsbericht ansehen (Seite 134)

Online-Sicherheitsbericht ansehen

Über den Bereich "Status des drahtlosen Netzwerks" können Sie einen Bericht über Ihre drahtlose Verbindung einsehen, egal ob diese sicher oder unsicher ist.

Die McAfee Wi-FiScan-Webseite zeigt Informationen über Ihre Sicherheitslücken im drahtlosen Netzwerk, Leistungsprobleme, Informationen über Ihre drahtlose Verbindung und eine empfohlene Sicherheitslösung an und stellt dar, ob Ihre Verbindung sicher ist.

Stellen Sie vor dem Einsehen des Sicherheitsberichts sicher, dass eine Verbindung zum Internet besteht.

So sehen Sie einen Online-Sicherheitsbericht über Ihr Netzwerk ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.
3. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" auf **Sicherheitsscan**.

   Nach dem Öffnen des Browsers müssen Sie eine ActiveX-Komponente herunterladen und installieren. Abhängig von den Einstellungen des Browsers kann es möglich sein, dass Ihr Browser das Steuerelement sperrt. Erlauben Sie Ihrem Browser das Herunterladen der

Komponente und führen Sie diese aus, um den Scan durchzuführen. In Abhängigkeit von der Geschwindigkeit Ihrer Internetverbindung kann der Scan einige Zeit dauern.

Hinweis: Weitere Informationen über das Herunterladen von ActiveX-Komponenten erhalten Sie in der Dokumentation Ihres Browsers.

McAfee Wi-FiScan unterstützt Internet Explorer 5.5 und höher.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 130)
- Verbindungsstatus ansehen (Seite 131)
- Netzwerksicherheitsmodus ansehen (Seite 133)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 133)
- Dauer der Netzwerkverbindung ansehen (Seite 133)
- Signalstärke des Netzwerks ansehen (Seite 134)

Geschützte drahtlose Netzwerke überwachen

Über Wireless Network Security können Sie im Bereich "Status des drahtlosen Netzwerks" die Anzahl der Verbindungen, Schlüsselrotationen und geschützten Computer einsehen. Weiterhin können Sie Netzwerkereignisse, den aktuellen Schlüssel und derzeit geschützte Computer einsehen.

Die folgende Tabelle beschreibt die Statusindikatoren für geschützte drahtlose Netzwerkverbindungen.

Status	Beschreibung	Informationen
Schlüsselrotationen heute	Zeigt die tägliche Anzahl der Schlüsselrotationen auf dem geschützten drahtlosen Netzwerk an.	Anzahl der Schlüsselrotationen einsehen (Seite 138)
Verbindungen heute	Zeigt die tägliche Anzahl der Verbindungen zum geschützten Netzwerk an.	Anzahl der täglichen Verbindungen ansehen (Seite 138)
In diesem Monat gesicherte Computer	Zeigt die Anzahl der Computer an, die im aktuellen Monat geschützt wurden.	Anzahl der monatlich geschützten Computer ansehen (Seite 138)
Netzwerke-ereignisse	Durch Klicken auf **Netzwerkereignisse** werden Ereignisse in Bezug auf Netzwerk, Verbindung und Schlüsselrotation angezeigt.	Geschützte drahtlose Netzwerkereignisse ansehen (Seite 139)

Status	Beschreibung	Informationen
Computer	Zeigt die Anzahl der Computer an, die mit dem geschützten drahtlosen Netzwerk verbunden sind, und wann die Verbindungen aufgehoben wurden.	Derzeit geschützte Computer ansehen (Seite 140)

Anzahl der Schlüsselrotationen einsehen

Über Wireless Network Security können Sie die tägliche Anzahl der Schlüsselrotationen ansehen, die auf Ihrem geschützten Netzwerk aufgetreten sind, und wann die letzte Schlüsselrotation durchgeführt wurde.

So sehen Sie die tägliche Anzahl Schlüsselrotationen ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Im Bereich "Status des drahtlosen Netzwerks" unter **Geschütztes drahtloses Netzwerk** im Feld **Schlüsselrotationen heute** werden die Gesamtanzahl der Verbindungen und die letzte Schlüsselrotation angezeigt.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 136)
- Anzahl der täglichen Verbindungen ansehen (Seite 138)
- Anzahl der monatlich geschützten Computer ansehen (Seite 138)
- Geschützte drahtlose Netzwerkereignisse ansehen (Seite 139)
- Derzeit geschützte Computer ansehen (Seite 140)
- Netzwerkschlüssel verwalten (Seite 119)
- Schlüssel automatisch rotieren (Seite 121)
- Netzwerkschlüssel manuell rotieren (Seite 125)

Anzahl der täglichen Verbindungen ansehen

Über Wireless Network Security können Sie die tägliche Anzahl der Verbindungen zum geschützten Netzwerk ansehen.

So sehen Sie die Verbindungen zum geschützten drahtlosen Netzwerk ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Im Bereich "Status des drahtlosen Netzwerks" unter **Geschütztes drahtloses Netzwerk** im Feld **Verbindungen heute** wird die Gesamtanzahl der Verbindungen angezeigt.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 136)
- Anzahl der monatlich geschützten Computer ansehen (Seite 138)
- Geschützte drahtlose Netzwerkereignisse ansehen (Seite 139)
- Derzeit geschützte Computer ansehen (Seite 140)

Anzahl der monatlich geschützten Computer ansehen

Über Wireless Network Security können Sie die Anzahl der Computer ansehen, die im aktuellen Monat geschützt sind.

So sehen Sie die Anzahl der Computer an, die im aktuellen Monat geschützt sind:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.
3. Im Bereich "Status des drahtlosen Netzwerks" unter **Geschütztes drahtloses Netzwerk** im Feld **In diesem Monat gesicherte Computer** wird die Anzahl der Computer angezeigt, die im aktuellen Monat geschützt sind.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 136)
- Anzahl der Schlüsselrotationen einsehen (Seite 138)
- Anzahl der täglichen Verbindungen ansehen (Seite 138)
- Geschützte drahtlose Netzwerkereignisse ansehen (Seite 139)
- Derzeit geschützte Computer ansehen (Seite 140)

Geschützte drahtlose Netzwerkereignisse ansehen

Wireless Network Security protokolliert Ereignisse auf dem drahtlosen Netzwerk; z. B. wenn Sicherheitsschlüssel rotiert werden, wenn andere Computer eine Verbindung zum McAfee-geschützten Netzwerk aufbauen und wenn sich andere Computer am McAfee-geschützten Netzwerk anmelden.

Über Wireless Network Security können Sie einen Bericht einsehen, der die Ereignisse beschreibt, die auf Ihrem Netzwerk eingetreten sind. Sie können die Arten der Ereignisse festlegen, die angezeigt werden sollen und Ereignisinformationen nach Datum, Ereignis oder Computer sortieren.

So sehen Sie Netzwerkereignisse an:

1 Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.

2 Führen Sie einen der folgenden Vorgänge aus:

Ziel	Aktion
Netzwerke- reignisse vom Bereich "Status des drahtlosen Netzwerks" aus ansehen	1. Wählen Sie **Status anzeigen** aus. 2. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" unter **Geschütztes drahtloses Netzwerk** auf **Netzwerkereignisse**.
Netzwerke- reignisse vom Bereich "Status des drahtlosen Netzwerks" aus ansehen	1. Klicken Sie auf **Tools anzeigen**. 2. Klicken Sie im Bereich "Extras" auf **Wartungstools**. 3. Klicken Sie im Bereich "Wartungstools" unter **Ereignisprotokoll anzeigen** auf **Anzeigen**.

3 Wählen Sie ein oder mehrere der folgenden Ereignisse zur Anzeige aus:

- **Netzwerkereignisse**: Zeigt Informationen über Netzwerkaktivitäten an; beispielsweise den Schutz eines drahtlosen Routers oder Zugriffspunkts.

- **Verbindungsereignisse**: Zeigt Informationen über Netzwerkverbindungen an; beispielsweise Datum und Zeit, zu denen ein Computer eine Verbindung zum Netzwerk aufgebaut hat.
- **Schlüsselrotationsereignisse**: Zeigt Informationen über die Daten und Zeiten der Sicherheitsschlüsselrotationen an.

4 Klicken Sie auf **Schließen**.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 136)
- Anzahl der Schlüsselrotationen einsehen (Seite 138)
- Anzahl der täglichen Verbindungen ansehen (Seite 138)
- Anzahl der täglichen Verbindungen ansehen (Seite 138)
- Derzeit geschützte Computer ansehen (Seite 140)

Derzeit geschützte Computer ansehen

Sie können die Anzahl der Computer ansehen, die mit dem geschützten drahtlosen Netzwerk verbunden sind, und wann jeweils deren letzte Verbindung stattfand.

So sehen Sie die Computer ein, die eine Verbindung zum geschützten Netzwerk aufgebaut haben:

1 Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.

2 Wählen Sie **Status anzeigen**.

3 Die Computer, die mit dem geschützten Netzwerk verbunden sind, als auch Zeit und Datum der jeweils letzten Verbindung werden im Bereich "Status des drahtlosen Netzwerks" unter **Computer** angezeigt.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 136)
- Anzahl der Schlüsselrotationen einsehen (Seite 138)
- Anzahl der täglichen Verbindungen ansehen (Seite 138)
- Anzahl der monatlich geschützten Computer ansehen (Seite 138)
- Geschützte drahtlose Netzwerkereignisse ansehen (Seite 139)

KAPITEL 18

Problembehandlung

Wenn Sie Wireless Network Security und Geräte von Fremdanbietern verwenden, können Sie Fehlerbehebungen vornehmen. Zu den behebbaren Problemen gehören:

- Installationsschwierigkeiten
- Schutz oder Konfiguration Ihres Netzwerks ist nicht möglich
- Verbindungsaufbau von Computern zum Netzwerk nicht möglich
- Verbindungsaufbau zu einem Netzwerk oder zum Internet nicht möglich
- Andere Probleme

In diesem Kapitel

Installieren von Wireless Network Security.....142
Schützen oder Konfigurieren des Netzwerks 144
Verbinden von Computern mit Ihrem Netzwerk.....147
Verbindung zum Internet und Netzwerk aufbauen .149
Andere Probleme.....155

Installieren von Wireless Network Security

Sie können die folgenden Installationsprobleme beheben:

- Auf welchen Computern muss diese Software installiert werden?
- Drahtloser Adapter wird nicht erkannt
- Mehrere drahtlose Adapter
- Kein Download auf drahtlose Computer möglich, da das Netzwerk bereits sicher ist

Auf welchen Computern muss diese Software installiert werden?

Installieren Sie Wireless Network Security auf allen drahtlosen Computern im Netzwerk (im Gegensatz zu anderen McAfee-Programmen können Sie diese Software auf mehreren Computern installieren). Befolgen Sie die Lizenzvereinbarung der erworbenen Software. In einigen Fällen kann es notwendig sein, zusätzliche Lizenzen zu erwerben.

Auf Computern ohne drahtlosen Adapter können Sie die Software installieren (müssen dies aber nicht tun). Auf diesen Computern ist die Software nicht aktiv, weil sie keinen entsprechenden Schutz benötigen.

Wireless Network Security wird derzeit von Windows XP oder Windows 2000 unterstützt.

Kompatibler drahtloser Adapter wird nicht erkannt

Wenn der drahtlose Adapter nach dem Installieren und Aktivieren nicht erkannt wird, müssen Sie den Computer neu starten. Wird der Adapter anschließend immer noch nicht erkannt, sollten Sie folgendermaßen vorgehen:

1. Öffnen Sie das Windows-Dialogfeld "Eigenschaften von Drahtlose Netzwerkverbindungen".
2. Klicken Sie unter Verwendung des klassischen Startmenüs von Windows auf **Start**, zeigen Sie auf **Einstellungen**, und wählen Sie **Netzwerkverbindungen** aus.
3. Klicken Sie auf das Symbol **Drahtlose Netzwerkverbindung**.
4. Klicken Sie im Dialogfeld "Status der drahtlosen Netzwerkverbindung" auf **Eigenschaften**.
5. Entfernen Sie im Bereich "Eigenschaften der drahtlosen Netzwerkverbindung" die Markierung für **MWL-Filter**, und nehmen Sie die Markierung erneut vor.

6. Klicken Sie auf **OK**.

   Sollte dieser Vorgang das Problem nicht behoben haben, führen Sie eine Prüfung mithilfe von Wi-FiScan durch. Wenn Wi-FiScan funktioniert, wird Ihr Adapter unterstützt. Wenn nicht, müssen Sie Ihren Adaptertreiber aktualisieren (über Windows-Aktualisierung, oder besuchen Sie die Webseite des Herstellers) oder einen neuen Treiber erwerben.

Verwandte Themen

- Online-Sicherheitsbericht ansehen (Seite 134)

Mehrere drahtlose Adapter

Wenn in einer Fehlermeldung steht, dass mehrere drahtlose Adapter installiert sind, müssen Sie alle bis auf einen deaktivieren oder vom Netzwerk trennen. Wireless Network Security funktioniert nur mit einem drahtlosen Adapter.

Download schlägt auf sicherem Netzwerk fehl

Installieren Sie, falls Sie über eine CD verfügen, Wireless Network Security von der CD auf allen drahtlosen Computern.

Wenn Sie die Software auf einem drahtlosen Computer installiert und das Netzwerk geschützt haben, bevor Sie die Software auf allen anderen Computern installiert haben, verfügen Sie über folgende Optionen.

- Heben Sie den Schutz des Netzwerks auf. Laden Sie dann die Software herunter, und installieren Sie sie auf allen drahtlosen Computern. Schützen Sie Ihr Netzwerk wieder.
- Zeigen Sie den Netzwerkschlüssel an. Geben Sie dann den Schlüssel auf Ihrem drahtlosen Computer ein, um eine Verbindung zum Netzwerk herzustellen. Laden Sie die Software herunter, installieren Sie diese, und melden Sie sich vom drahtlosen Computer aus am Netzwerk an.
- Laden Sie die ausführbare Datei auf den Computer herunter, der bereits mit dem Netzwerk verbunden ist, und speichern Sie diese auf einem USB-Flash-Laufwerk, oder brennen Sie sie auf eine CD, damit Sie sie auf den anderen Computern installieren können.
- Führen Sie die Windows Connect Now-Technologie aus.

Verwandte Themen

- Drahtlose Router oder Zugriffspunkte entfernen (Seite 109)
- Aktuelle Schlüssel anzeigen (Seite 120)
- Hinzufügen von Computern über Wechselgeräte (Seite 95)
- Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie (Seite 97)

Schützen oder Konfigurieren des Netzwerks

Sie können die folgenden Probleme in Bezug auf den Schutz und die Konfiguration Ihres Netzwerks beheben:

- Nicht unterstützter Router oder Zugriffspunkt
- Aktualisieren der Firmware des Routers oder Zugriffspunkts
- Fehler durch doppelte Administratoren
- Netzwerk als ungesichert angezeigt
- Keine Reparatur möglich

Nicht unterstützter Router oder Zugriffspunkt

Wenn es in einer Fehlermeldung heißt, dass der drahtlose Router oder Zugriffspunkt unter Umständen nicht unterstützt wird, konnte das Gerät von Wireless Network Security nicht konfiguriert werden, weil es nicht erkannt oder gefunden wurde.

Stellen Sie durch Anforderung eines Updates sicher, dass Sie über die neueste Version von Wireless Network Security verfügen (McAfee weitet die Unterstützung ständig auf neue Router und Zugriffspunkte aus). Wenn der Router oder Zugriffspunkt in der Liste der unterstützten Router aufgeführt wird und dieser Fehler dennoch auftritt, liegen Kommunikationsprobleme zwischen Ihrem Computer und dem Router oder Zugriffspunkt vor.

Verwandte Themen

- Unterstützte drahtlose Router
  http://www.mcafee.com/router

Aktualisieren der Firmware des Routers oder Zugriffspunkts

Wenn es in einer Fehlermeldung heißt, dass die Firmware-Version des drahtlosen Routers oder Zugriffspunkts nicht unterstützt wird, wird zwar das Gerät unterstützt, nicht aber dessen Firmware-Version. Stellen Sie durch Anforderung eines Updates sicher, dass Sie über die neueste Version von Wireless Network Security verfügen (McAfee weitet die Unterstützung ständig auf neue Firmware-Versionen aus).

Wenn Sie über die neueste Version von Wireless Network Security verfügen, sollten Sie die Website des Herstellers des Routers oder Zugriffspunkts aufrufen bzw. sich an dessen Support wenden und eine in der Liste unterstützter Router aufgelistete Firmware-Version installieren.

Verwandte Themen

- Unterstützte drahtlose Router
  http://www.mcafee.com/router

Fehler durch doppelte Administratoren

Nach dem Konfigurieren des Routers oder Zugriffspunkts müssen Sie sich von der Administrationsoberfläche abmelden. Geschieht das nicht, verhält der Router oder Zugriffspunkt sich in einigen Fällen so, als würde er weiterhin von einem anderen Computer konfiguriert werden. Es wird dann eine Fehlermeldung angezeigt.

Wenn Sie sich nicht abmelden können, ziehen Sie das Stromkabel Ihres Routers oder Zugriffspunkts heraus, und stecken Sie es dann wieder ein.

Fehler bei der Schlüsselrotation

Fehlerursache:

- Die Anmeldeinformationen für Ihren Router oder Zugriffspunkt wurden geändert.
- Die Firmware-Version Ihres Routers oder Zugriffspunkts wurde geändert, und die neue Version wird nicht unterstützt.
- Ihr Router oder Zugriffspunkt ist nicht verfügbar. Stellen Sie sicher, dass der Router oder Zugriffspunkt eingeschaltet und an das Netzwerk angeschlossen ist.
- Fehler durch doppelte Administratoren.
- Bei einigen drahtlosen Routern kann es vorkommen, dass der McAfee-Client nicht in der Lage ist, auf das Management Interface zuzugreifen, um den Verschlüsselungsschlüssel zu rotieren, wenn bereits ein anderer Computer auf der Weboberfläche des drahtlosen Routers manuell angemeldet ist.

Verwandte Themen

- Informationen für drahtlose Geräte ändern (Seite 117)
- Schlüssel automatisch rotieren (Seite 121)

Reparieren des Routers oder Zugriffspunkts nicht möglich

Gehen Sie folgendermaßen vor, wenn bei der Reparatur Fehler auftreten. Beachten Sie, dass die einzelnen Verfahren voneinander unabhängig sind.

- Stellen Sie per Kabel eine Verbindung zu Ihrem Netzwerk her, und wiederholen Sie dann den Reparaturvorgang.
- Ziehen Sie das Stromkabel des Routers oder Zugriffspunkts, und stecken Sie es dann wieder ein. Versuchen Sie dann, eine Verbindung herzustellen.
- Setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und reparieren Sie ihn. Hierdurch werden die drahtlosen Einstellungen auf die Standardeinstellungen zurückgesetzt. Setzen Sie dann die Einstellungen für Ihre Internetverbindung zurück.
- Verlassen Sie mithilfe der erweiterten Optionen das Netzwerk auf allen Computern, setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und schützen Sie ihn dann. Hierdurch werden die drahtlosen Einstellungen auf die Standardeinstellungen zurückgesetzt. Setzen Sie dann die Einstellungen für Ihre Internetverbindung zurück.

Verwandte Themen

- Netzwerk-Sicherheitseinstellungen reparieren (Seite 118)

Netzwerk scheint ungeschützt

Wenn das Netzwerk als ungesichert angezeigt wird, ist es nicht geschützt. Sie müssen das Netzwerk schützen. Beachten Sie, dass Wireless Network Security ausschließlich mit kompatiblen Routern und Zugriffspunkten funktionsfähig ist.

Verwandte Themen

- Geschützte drahtlose Netzwerke erstellen (Seite 84)
- Unterstützte drahtlose Router
  http://www.mcafee.com/router

Verbinden von Computern mit Ihrem Netzwerk

Sie können die folgenden Probleme in Bezug auf die Verbindung von Computern zum Netzwerk beheben:

- Warten auf Autorisierung
- Gewähren von Zugriff für einen unbekannten Computer

Warten auf Autorisierung

Wenn Sie sich an einem geschützten Netzwerk anzumelden versuchen und der Computer vergeblich auf Autorisierung wartet, sollten Sie Folgendes überprüfen.

- Ein drahtloser Computer mit bestehendem Zugriff auf das Netzwerk ist eingeschaltet und mit dem Netzwerk verbunden.
- An diesem Computer ist jemand anwesend, der Zugriff erteilen kann, wenn Ihr Computer angezeigt wird.
- Die Computer befinden sich innerhalb der Reichweite der Funkwellen.

Wenn **Zugriff gewähren** auf dem Computer mit bestehendem Zugriff auf das Netzwerk nicht angezeigt wird, müssen Sie versuchen, den Zugriff von einem anderen Computer aus zu gewähren.

Falls keine anderen Computer verfügbar sind, müssen Sie den Schutz des Netzwerks vom Computer mit vorhandenem Zugriff aus aufheben und das Netzwerk vom Computer ohne Zugriff aus schützen. Melden Sie sich anschließend von dem Computer aus am Netzwerk an, der das Netzwerk ursprünglich schützte.

Weiterhin können Sie die Funktion "Anderen Computer schützen" verwenden.

Verwandte Themen

- Anmelden an einem geschützten drahtlosen Netzwerk (Seite 86)
- Geschützte drahtlose Netzwerke verlassen (Seite 112)
- Drahtlose Router oder Zugriffspunkte entfernen (Seite 109)
- Computer zum geschützten drahtlosen Netzwerk hinzufügen (Seite 95)

Gewähren von Zugriff für einen unbekannten Computer

Wenn Sie von einem unbekannten Computer eine Anfrage auf die Gewährung von Zugriff erhalten, sollten Sie diese ablehnen, bis dessen Legitimität bestätigt ist. Möglicherweise versucht ein Unbefugter, auf Ihr Netzwerk zuzugreifen.

Verbindung zum Internet und Netzwerk aufbauen

Sie können die folgenden Probleme in Bezug auf die Verbindung zu einem Netzwerk oder zum Internet beheben:

- Schlechte Verbindung zum Internet
- Kurze Unterbrechung der Verbindung
- Verbindungsverlust bei Geräten (nicht beim Computer)
- Aufforderung zur Eingabe des WEP-, WPA- oder WPA2-Schlüssels
- Keine Verbindung möglich
- Aktualisieren des drahtlosen Adapters
- Schwaches Signal
- Windows kann die drahtlose Verbindung nicht konfigurieren
- Windows zeigt keine Verbindung an

Verbindung zum Internet kann nicht hergestellt werden

Wenn Sie keine Verbindung herstellen können, schließen Sie den Computer mit einem Kabel an das Netzwerk an, und stellen Sie dann eine Verbindung zum Internet her. Ist immer noch keine Verbindung möglich, sollten Sie die folgenden Punkte überprüfen:

- Ihr Modem ist eingeschaltet
- Ihre PPPoE-Einstellungen sind korrekt
- Ihre DSL- oder Kabelleitung ist aktiv

Verbindungsprobleme, etwa mit der Geschwindigkeit und der Signalstärke, können auch durch Funkstörungen verursacht werden. Versuchen Sie das Problem über die folgenden Methoden zu beheben:

- Ändern Sie den Kanal des schnurlosen Telefons.
- Beseitigen Sie mögliche Störquellen.
- Ändern Sie den Standort des drahtlosen Routers, Zugriffspunkts oder Computers.
- Ändern Sie den Kanal von Router oder Zugriffspunkt. Die Kanäle 1, 4, 7 und 11 werden für Nord- und Südamerika empfohlen. Die Kanäle 1, 4, 7, 13 werden für die anderen Länder empfohlen. Viele Router sind standardmäßig auf Kanal 6 eingestellt.
- Stellen Sie sicher, dass weder Router noch drahtloser Adapter (insbesondere ein drahtloser USB-Adapter) nicht gegen eine Wand eingerichtet sind.
- Stellen Sie sicher, dass sich Ihr drahtloser USB-Adapter nicht neben einem drahtlosen AP/Router befindet.
- Stellen Sie den Router entfernt von Wänden und metallischen Gegenständen auf.

Verbindung unterbrochen

Wenn Ihre Verbindung kurzzeitig unterbrochen wird (z. B. während eines Online-Spiels), kann eine Schlüsselrotation die Ursache hierfür sein. Um dies zu verhindern, können Sie die Schlüsselrotation aussetzen.

Sie sollten die Schlüsselrotation möglichst bald fortsetzen, damit das Netzwerk vor Hackern vollständig geschützt ist.

Verwandte Themen

- Schlüssel automatisch rotieren (Seite 121)
- Schlüsselrotation fortsetzen (Seite 122)
- Automatische Schlüsselrotation aussetzen (Seite 124)
- Netzwerkschlüssel manuell rotieren (Seite 125)

Verbindungsverlust bei Geräten

Wenn einige Geräte die Verbindung verlieren, während Wireless Network Security eingesetzt wird, versuchen Sie das Problem durch eine der folgenden Methoden zu beheben:

- Setzen Sie die Schlüsselrotation aus
- Aktualisieren Sie den Treiber für den drahtlosen Adapter
- Deaktivieren Sie den Client-Manager des Adapters

Verwandte Themen

- Automatische Schlüsselrotation aussetzen (Seite 124)

Aufforderung zur Eingabe des WEP-, WPA- oder WPA2-Schlüssels

Wenn Sie zum Herstellen einer Verbindung zum geschützten drahtlosen Netzwerk einen WEP-, WPA- oder WPA2-Schlüssel eingeben müssen, haben Sie wahrscheinlich die Software nicht auf Ihrem Computer installiert.

Für eine ordnungsgemäße Funktionsweise muss Wireless Network Security auf allen drahtlosen Computern im Netzwerk installiert sein.

Verwandte Themen

- Wireless Network Security starten (Seite 78)
- Computer zum geschützten drahtlosen Netzwerk hinzufügen (Seite 95)

Verbindung zum drahtlosen Netzwerk nicht möglich

Wenn Sie keine Verbindung herstellen können, gehen Sie folgendermaßen vor: Beachten Sie, dass die einzelnen Verfahren voneinander unabhängig sind.

- Vergewissern Sie sich, falls Sie keine Verbindung zu einem geschützten Netzwerk herstellen, dass Sie über den richtigen Schlüssel verfügen. Geben Sie ihn erneut ein.
- Ziehen Sie den Stecker des drahtlosen Adapters, und stecken Sie ihn wieder ein. Oder deaktivieren Sie den Adapter, und aktivieren Sie ihn dann wieder.
- Schalten Sie den Router oder Zugriffspunkt aus und wieder ein. Versuchen Sie dann, eine Verbindung herzustellen.
- Vergewissern Sie sich, dass der drahtlose Router oder Zugriffspunkt verbunden ist, und reparieren Sie die Sicherheitseinstellungen.
- Starten Sie den Computer neu.
- Aktualisieren Sie den drahtlosen Adapter, oder erwerben Sie einen neuen. Beispiel: Ihr Netzwerk setzt WPA-PSK

TKIP-Sicherheit ein, und Ihr drahtloser Adapter unterstützt den Sicherheitsmodus des Netzwerks nicht (die Netzwerke zeigen WEP an, obwohl sie auf WPA festgelegt sind).

- Wenn Sie nach dem Aktualisieren des drahtlosen Routers oder Zugriffspunkts keine Verbindung herstellen können, haben Sie möglicherweise auf eine nicht unterstützte Version aktualisiert. Vergewissern Sie sich, dass der Router oder Zugriffspunkt unterstützt wird. Wenn dies nicht der Fall ist, sollten Sie eine unterstützte Version installieren oder warten, bis ein Update von Wireless Network Security verfügbar ist.

Verwandte Themen

- Netzwerk-Sicherheitseinstellungen reparieren (Seite 118)
- Aktualisieren des drahtlosen Adapters (Seite 152)

Aktualisieren des drahtlosen Adapters

Eventuell müssen Sie Ihren drahtlosen Adapter aktualisieren, um Wireless Network Security verwenden zu können.

So aktualisieren Sie Ihren Adapter:

1. Klicken Sie auf dem Desktop auf **Start**, zeigen Sie auf **Einstellungen**, und wählen Sie dann **Systemsteuerung** aus.
2. Doppelklicken Sie auf das Symbol **System**. Das Dialogfeld **Systemeigenschaften** wird angezeigt.
3. Wählen Sie die Registerkarte **Hardware** aus, und klicken Sie dann auf **Geräte-Manager**.
4. Doppelklicken Sie in der Liste **Geräte-Manager** auf Ihren Adapter.
5. Wählen Sie die Registerkarte **Treiber** aus, und notieren Sie sich den Treiber, der bei Ihnen installiert ist.
6. Besuchen Sie die Webseite des Adapterherstellers, um nach einer Aktualisierung zu suchen. Treiber sind meist im Support- oder Download-Bereich zu finden. Wenn Sie eine Mini-PCI-Karte verwenden, gehen Sie zur Webseite des Herstellers des Computers und nicht des Kartenherstellers.
7. Wenn ein Treiber-Update verfügbar ist, folgen Sie den Anweisungen auf der Website, um das Update herunterzuladen.
8. Gehen Sie zurück zur Registerkarte **Treiber**, und klicken Sie auf **Aktualisieren**. Ein Windows-Assistent wird angezeigt.
9. Befolgen Sie die Anweisungen auf der Webseite, um den Treiber zu installieren.

Schwaches Signal

Wenn Ihre Verbindung unterbrochen wird oder sehr langsam ist, ist möglicherweise das Signal zu schwach. Gehen Sie wie folgt vor, um das Signal zu verbessern:

- Stellen Sie sicher, dass die drahtlosen Geräte nicht durch Metallobjekte wie Öfen, Rohre oder große Haushaltsgeräte blockiert werden. Funksignale werden stark abgeschwächt, wenn sie durch solche Objekte hindurch verlaufen.
- Wenn das Signal durch Wände gelangen muss, sollten Sie sicherstellen, dass dies nicht im spitzen Winkel geschieht. Je länger der Weg innerhalb der Wand ist, desto schwächer wird das Signal.
- Verfügt der drahtlose Router oder Zugriffspunkt über zwei Antennen, sollten Sie die beiden Antennen nach Möglichkeit rechtwinklig zueinander ausrichten (eine vertikal und eine horizontal im 90-Grad-Winkel).
- Einige Hersteller verwenden Hochleistungsantennen. Richtantennen haben eine größere Reichweite, während omnidirektionale Antennen (Rundstrahler) die größte Flexibilität bieten. Richten Sie sich beim Installieren der Antenne nach den entsprechenden Anweisungen des Herstellers.

Führen diese Schritte nicht zum Erfolg, sollten Sie dem Netzwerk einen Zugriffspunkt hinzufügen, der sich näher an dem Computer befindet, zu dem Sie eine Verbindung herstellen möchten. Wenn Sie den zweiten Zugriffspunkt mit demselben Netzwerknamen (SSID) und einem anderen Kanal konfigurieren, sucht der Adapter automatisch das stärkste Signal und stellt die Verbindung über den entsprechenden Zugriffspunkt her.

Verwandte Themen

- Signalstärkensymbole (Seite 101)
- Signalstärke des Netzwerks ansehen (Seite 134)

Windows unterstützt keine drahtlose Verbindung

Wenn Sie eine Windows-Meldung darauf hinweist, dass die drahtlose Verbindung nicht konfiguriert werden kann, können Sie diese Meldung ignorieren. Verwenden Sie Wireless Network Security, um Verbindungen zu drahtlosen Netzwerken herzustellen und die Netzwerke zu konfigurieren.

Stellen Sie sicher, dass im Windows-Dialogfeld "Eigenschaften von Drahtlose Netzwerkverbindung" auf der Registerkarte "Drahtlosnetzwerke" das Kontrollkästchen **Windows zum Konfigurieren der Einstellungen verwenden** deaktiviert ist.

Wireless Network Security ermöglicht folgende Dinge:

- Adapter, die an Computern mit Windows 2000 installiert sind, können eine Verbindung zu WPA-Netzwerken aufbauen, auch wenn der Karten-Client-Manager nicht unterstützt wird.
- Adapter an Computern, auf denen Windows XP läuft, können eine Verbindung zu WPA2-Netzwerken aufbauen, ohne dass der Win XP SP2-Hotfix installiert werden muss.
- Adapter unter Windows XP SP1 können eine Verbindung zu WPA- und WPA2-Netzwerken aufbauen, ohne dass ein Hotfix installiert werden muss, der nicht von Windows XP SP1 unterstützt wird.

Windows zeigt keine Verbindung an

Wenn Sie verbunden sind, das Netzwerksymbol von Windows jedoch ein X anzeigt (d. h. keine Verbindung), so können Sie das ignorieren. Ihre Verbindung ist einwandfrei.

Andere Probleme

Sie können die folgenden Probleme beheben:

- Bei Verwendung anderer Programme lautet der Netzwerkname anders
- Probleme beim Konfigurieren drahtloser Router oder Zugriffspunkte
- Ersetzen von Computern
- Auswahl eines anderen Sicherheitsmodus
- Software funktioniert nach dem Aktualisieren des Betriebssystems nicht

Bei Verwendung anderer Programme lautet der Netzwerkname anders

Dass der Name des Netzwerks in anderen Programmen anders angezeigt wird (etwa mit _SafeAaf als Bestandteil des Namens), ist völlig normal.

Wireless Network Security kennzeichnet Netzwerke mit einem Code, wenn sie geschützt sind.

Drahtlose Router oder Zugriffspunkte konfigurieren

Wenn beim Konfigurieren des Routers oder Zugriffspunkts oder beim Hinzufügen mehrerer Router im Netzwerk ein Fehler auftritt, müssen Sie sich vergewissern, dass alle Router und Zugriffspunkte über eine eigene IP-Adresse verfügen.

Wenn der Name des drahtlosen Routers oder Zugriffspunkts im Dialogfeld "Drahtlosen Router/Zugriffspunkt schützen" aufgeführt wird, Sie jedoch bei dessen Konfiguration eine Fehlermeldung erhalten, müssen Sie überprüfen, ob der Router oder Zugriffspunkt unterstützt wird.

Wenn der Router oder Zugriffspunkt konfiguriert ist, sich aber scheinbar nicht im richtigen Netzwerk befindet (es werden zum Beispiel keine anderen Computer im LAN angezeigt), müssen Sie sicherstellen, dass Sie den richtigen Router oder Zugriffspunkt konfiguriert haben, und nicht den Ihres Nachbarn. Ziehen Sie das Stromkabel des Routers oder Zugriffspunkts, und vergewissern Sie sich, dass die Verbindung unterbrochen wird. Wenn Sie den falschen Router oder Zugriffspunkt konfiguriert haben, heben Sie dessen Schutz wieder auf, und schützen Sie dann den richtigen Router oder Zugriffspunkt.

Wenn Sie den Router oder Zugriffspunkt nicht ordnungsgemäß konfigurieren oder hinzufügen können, er aber unterstützt wird, liegt das unter Umständen daran, dass Sie Änderungen durchgeführt haben, die nun eine ordnungsgemäße Konfiguration verhindern.

- Folgen Sie den Anweisungen des Herstellers zum Konfigurieren Ihres drahtlosen Routers bzw. Zugriffspunkts für DHCP oder zum Festlegen der richtigen IP-Adresse. In einigen Fällen ist ein Konfigurations-Tool im Lieferumfang des Produkts enthalten.
- Setzen Sie den Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und versuchen Sie erneut, das Netzwerk zu reparieren. Möglicherweise haben Sie den Administrationsport am Router oder Zugriffspunkt geändert oder die drahtlose Administration deaktiviert. Stellen Sie sicher, dass Sie die Standardkonfiguration verwenden und dass die drahtlose Konfiguration aktiviert ist. Eine weitere Möglichkeit besteht darin, dass die http-Administration deaktiviert ist. Stellen Sie in diesem Fall sicher, dass sie aktiviert ist. Stellen Sie sicher, dass Sie Port 80 für die Administration verwenden.
- Wenn der drahtlose Router oder Zugriffspunkt nicht in der Liste drahtloser Router oder Zugriffspunkte aufgeführt wird, die geschützt und zu denen Verbindungen hergestellt werden sollen, müssen Sie die SSID-Übertragung aktivieren und sicherstellen, dass Ihr Router oder Zugriffspunkt in der Liste der verfügbaren Netzwerke von Wireless Network Security aufgelistet ist.

- Falls Sie getrennt werden oder keine Verbindung herstellen können, ist möglicherweise die MAC-Filterung aktiviert. Deaktivieren Sie sie.
- Wenn zwischen zwei Computern mit drahtloser Verbindung zum Netzwerk keine Netzwerkvorgänge möglich sind (zum Beispiel die Freigabe von Dateien oder das Drucken auf freigegebenen Druckern), müssen Sie überprüfen, ob die Isolierung von Zugriffspunkten nicht aktiviert ist. Sie verhindert, dass drahtlose Computer über das Netzwerk miteinander in Verbindung treten können.
- Wenn Sie eine andere Firewall als die McAfee Personal Firewall verwenden, müssen Sie sicherstellen, dass das Subnet vertrauenswürdig ist.

Verwandte Themen

- Unterstützte drahtlose Router
  http://www.mcafee.com/router

Ersetzen von Computern

Wenn der Computer, der das Netzwerk geschützt hat, ersetzt wurde und es keine anderen Computer mit Zugriff gibt (d. h. Sie können nicht auf das Netzwerk zugreifen), setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und schützen Sie das Netzwerk erneut.

Auswahl eines anderen Sicherheitsmodus

Wenn eine Fehlermeldung darauf hinweist, dass Sie einen Sicherheitsmodus ausgewählt haben, der vom drahtlosen Adapter nicht unterstützt wird, müssen Sie einen anderen Sicherheitsmodus auswählen.

- Alle Adapter unterstützen WEP.
- Die meisten Adapter, die WPA unterstützen, verwenden sowohl WPA-PSK TKIP- als auch WPA-PSK AES-Sicherheitsmodi.
- Adapter, die WPA2 unterstützen, verwenden WPA-Sicherheitsmodi und WPA2-PSK TKIP, WPA2-PSK AES und WPA2-PSK TKIP/AES.

Verwandte Themen

- Konfigurieren von Sicherheitseinstellungen (Seite 114)
- Netzwerksicherheitsmodus ansehen (Seite 132)

Software funktioniert nach Aktualisierung des Betriebssystems nicht

Wenn Wireless Network Security nach der Aktualisierung von Betriebssystemen nicht funktionieren sollte, entfernen Sie das Programm, und installieren Sie es neu.

KAPITEL 19

McAfee EasyNetwork

McAfee(R) EasyNetwork ermöglicht sichere Dateifreigabe, vereinfachte Dateiübertragungen und automatische Druckerfreigabe für die Computer in Ihrem privaten Netzwerk.

Bevor Sie mit der Verwendung von EasyNetwork beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu EasyNetwork.

In diesem Kapitel

Funktionen 160
EasyNetwork einrichten 161
Dateien freigeben und senden 169
Drucker freigeben 175

Funktionen

EasyNetwork bietet folgende Funktionen:

Dateifreigabe

EasyNetwork vereinfacht die Dateifreigabe auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden.

Dateiübertragung

Sie können Dateien an andere Computer senden, die Mitglied des verwalteten Netzwerks sind. Wenn Sie eine Datei empfangen, wird diese in Ihrem EasyNetwork-Eingangsbereich angezeigt. Der Eingangsbereich ist ein temporärer Speicherort für alle Dateien, die andere Computer im Netzwerk an Sie senden.

Automatisierte Druckerfreigabe

Wenn Sie Mitglied eines verwalteten Netzwerks werden, gibt EasyNetwork automatisch alle lokalen Drucker frei, die an Ihren Computer angeschlossen sind. Dabei verwendet es für den Namen der Druckerfreigabe den aktuellen Namen des Druckers. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden.

KAPITEL 20

EasyNetwork einrichten

Bevor Sie die EasyNetwork-Funktionen verwenden können, müssen Sie das Programm starten und sich beim verwalteten Netzwerk anmelden. Nach der Anmeldung können Sie das Netzwerk jederzeit wieder verlassen.

In diesem Kapitel

Starten von EasyNetwork 162
Anmelden an einem verwalteten Netzwerk 163
Verwaltetes Netzwerk verlassen 167

Starten von EasyNetwork

Standardmäßig werden Sie direkt nach der Installation von EasyNetwork gefragt, ob Sie das Programm starten möchten; Sie können EasyNetwork jedoch auch später starten.

EasyNetwork starten

Sie werden standardmäßig aufgefordert, EasyNetwork direkt nach der Installation zu starten. Sie können es jedoch auch zu einem späteren Zeitpunkt starten.

So starten Sie EasyNetwork:

- Klicken Sie im Menü **Start** auf **Programme**, **McAfee** und anschließend auf **McAfee EasyNetwork**.

Tipp: Wenn Sie während der Installation das Erstellen von Desktop- und Schnellstartsymbolen gewählt haben, können Sie EasyNetwork auch starten, indem Sie auf dem Desktop auf das McAfee EasyNetwork-Symbol doppelklicken oder indem Sie im Benachrichtigungsbereich rechts neben der Taskleiste auf das McAfee EasyNetwork-Symbol klicken.

Anmelden an einem verwalteten Netzwerk

Nach der Installation von SecurityCenter wird Ihrem Computer ein Netzwerkagent hinzugefügt, der im Hintergrund ausgeführt wird. In EasyNetwork ist der Netzwerkagent verantwortlich für das Finden einer gültigen Netzwerkverbindung, das Finden lokaler Drucker zur Freigabe und das Überwachen des Netzwerkstatus.

Wenn in dem Netzwerk, in dem Sie sich derzeit befinden, kein anderer Computer gefunden wird, der den Netzwerkagenten ausführt, werden Sie automatisch zu einem Mitglied dieses Netzwerks gemacht und müssen angeben, ob das Netzwerk vertrauenswürdig ist. Da Ihr Computer der erste ist, der dem Netzwerk beitritt, erscheint der Name Ihres Computers als Teil des Netzwerknamens; Sie können das Netzwerk jedoch jederzeit umbenennen.

Wenn ein Computer eine Verbindung mit dem Netzwerk herstellt, wird an alle anderen Computer, die sich bereits im Netzwerk verbinden, eine Beitrittsanfrage gesendet. Diese Anfrage kann von jedem Computer genehmigt werden, der über administrative Berechtigung für das Netzwerk verfügt. Der Computer, der Zugriff gewährt, kann die Berechtigungsstufe für den Computer festlegen, der gerade dem Netzwerk beitritt; beispielsweise Gast (nur Dateiübertragung) oder vollständig/administrativ (Dateiübertragung und Dateifreigabe). In EasyNetwork können Computer mit administrativem Zugriff anderen Computern Zugriff gewähren und Berechtigungen verwalten (d. h. Computer mit mehr oder weniger Rechten versehen); Computer mit vollständigem Zugriff können diese administrativen Aufgaben nicht ausführen. Bevor der Computer dem Netzwerk beitreten darf, wird außerdem eine Sicherheitsüberprüfung durchgeführt.

Hinweis: Wenn Sie andere Netzwerkprogramme von McAfee installiert haben (z. B. McAfee Wireless Network Security oder Network Manager), wird der Computer nach dem Beitritt auch in diesen Programmen als verwalteter Computer erkannt. Die Berechtigungsstufe, die einem Computer zugewiesen wird, gilt für alle McAfee-Netzwerkprogramme. Weitere Informationen dazu, was Gastberechtigungen, vollständige oder administrative Berechtigungen in anderen McAfee-Netzwerkprogrammen bedeuten, finden Sie in der Dokumentation zu dem jeweiligen Programm.

Dem Netzwerk beitreten

Wenn ein Computer zum ersten Mal nach der Installation von EasyNetwork einem vertrauenswürdigen Netzwerk beitritt, wird der Benutzer gefragt, ob er dem verwalteten Netzwerk beitreten möchte. Wenn der Benutzer des Computers dem Beitritt zustimmt, wird an alle anderen Computer im Netzwerk, die über administrativen Zugriff verfügen, eine Anfrage gesendet. Diese Anfrage muss genehmigt werden, bevor der Computer Drucker oder Dateien freigeben oder Dateien im Netzwerk senden oder kopieren kann. Wenn der Computer der erste Computer im Netzwerk ist, werden ihm automatisch administrative Genehmigungen verliehen.

So treten Sie dem Netzwerk bei:

1. Klicken Sie im Fenster "Freigegebene Dateien" auf **Ja, diesem Netzwerk jetzt beitreten**.
   Wenn ein administrativer Computer im Netzwerk Ihre Anfrage genehmigt, wird eine Nachricht angezeigt, in der festgelegt werden muss, ob dieser Computer und andere Computer im Netzwerk die Sicherheitseinstellungen der jeweils anderen Computer verwalten dürfen.
2. Wen dieser Computer und andere Computer im Netzwerk die Sicherheitseinstellungen der jeweils anderen Computer verwalten sollen, klicken Sie auf **Ja**; klicken Sie andernfalls auf **Nein**.
3. Bestätigen Sie, dass der Computer, der den Netzwerkzugriff gewährt, die Spielkarten anzeigt, die derzeit im Dialogfeld für die Bestätigung der Sicherheit angezeigt werden, und klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer, der Ihnen den Zugriff gewährt hat, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Anmelden am Netzwerk ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Zugriff auf das Netzwerk gewähren

Wenn ein Computer dem verwalteten Netzwerk beitreten möchte, wird den anderen Computern im Netzwerk, die über administrativen Zugriff verfügen, eine Nachricht gesendet. Der erste Computer, der auf diese Nachricht antwortet, ist der Computer, der Zugriff gewährt. Der Computer, der Zugriff gewährt, entscheidet, welche Art von Zugriff dem Computer gewährt wird: Gast, vollständig oder administrativ

So gewähren Sie Zugriff auf das Netzwerk:

1. Aktivieren Sie in der Nachricht eines der folgenden Kontrollkästchen:
   - **Zugriff als Gast gewähren**: Der Benutzer kann Dateien an andere Computer senden, aber keine Dateien freigeben.
   - **Vollständigen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**: Der Benutzer kann Dateien senden und freigeben.
   - **Administrativen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**: Der Benutzer kann Dateien senden und freigeben, anderen Computern Zugriff gewähren und die Berechtigungsstufen anderer Computer anpassen.
2. Klicken Sie auf **Zugriff gewähren**.
3. Bestätigen Sie, dass der Computer die Spielkarten anzeigt, die derzeit im Dialogfeld für die Bestätigung der Sicherheit angezeigt werden, und klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Gewähren des Zugriffs für diesen Computer ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Netzwerk umbenennen

Standardmäßig beinhaltet der Netzwerkname den Namen des ersten Computers, der dem Netzwerk beigetreten ist; Sie können den Netzwerknamen jedoch jederzeit ändern. Wenn Sie den Netzwerknamen ändern, können Sie die Netzwerkbeschreibung ändern, die in EasyNetwork angezeigt wird.

So benennen Sie das Netzwerk um:

1. Klicken Sie im Menü **Optionen** auf **Konfiguration**.
2. Geben Sie im Dialogfeld "Konfiguration" den Namen des Netzwerks in das Feld **Netzwerkname** ein.
3. Klicken Sie auf **OK**.

Verwaltetes Netzwerk verlassen

Wenn Sie sich bei einem verwalteten Netzwerk anmelden und anschließend entscheiden, dass Sie nicht länger Mitglied dieses Netzwerks sein möchten, können Sie das Netzwerk verlassen. Wenn Sie Ihre Mitgliedschaft aufgegeben haben, können Sie sich jederzeit wieder anmelden. Ihnen muss jedoch die Berechtigung zum Anmelden gewährt und die Sicherheitsprüfung muss erneut ausgeführt werden. Weitere Informationen finden Sie unter Bei einem verwalteten Netzwerk anmelden (Seite 163).

Verwaltetes Netzwerk verlassen

Sie können ein verwaltetes Netzwerk verlassen, bei dem Sie sich zuvor angemeldet haben.

So verlassen Sie ein verwaltetes Netzwerk:

1. Klicken Sie im Menü **Tools** auf **Netzwerk verlassen**.
2. Wählen Sie im Dialogfeld "Netzwerk verlassen" den Namen des Netzwerks, das Sie verlassen möchten.
3. Klicken Sie auf **Netzwerk verlassen**.

KAPITEL 21

Dateien freigeben und senden

EasyNetwork vereinfacht das Freigeben und Senden von Dateien auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden.

In diesem Kapitel

Dateien freigeben.....170
Senden von Dateien an andere Computer.....173

Dateien freigeben

EasyNetwork vereinfacht die Dateifreigabe auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden. Wenn Sie einen Ordner freigeben, werden alle darin und in den Unterordnern enthaltenen Dateien freigegeben. Nachträglich hinzugefügte Dateien werden jedoch nicht automatisch freigegeben. Wenn eine freigegebene Datei oder ein freigegebener Ordner gelöscht wird, wird sie bzw. er automatisch aus dem Fenster "Freigegebene Dateien" entfernt. Sie können eine Dateifreigabe jederzeit rückgängig machen.

Sie haben zwei Möglichkeiten, auf eine freigegebene Datei zuzugreifen: indem Sie die Datei direkt in EasyNetwork öffnen oder sie auf Ihren Computer kopieren und sie dann öffnen. Wenn Ihre Liste der Dateifreigaben zu lang ist, können Sie nach der freigegebenen Datei suchen, auf die Sie zugreifen möchten.

Hinweis: Auf Dateien, die über EasyNetwork freigegeben wurden, kann von anderen Computern mit Windows-Explorer nicht zugegriffen werden. Das Freigeben von Dateien über EasyNetwork erfolgt über sichere Verbindungen.

Freigabe einer Datei

Wenn Sie eine Datei freigeben, können automatisch alle anderen Mitglieder mit vollständigem oder administrativem Zugriff auf das verwaltete Netzwerk darauf zugreifen.

So geben Sie eine Datei frei:

1. Finden Sie in Windows-Explorer die Datei, die Sie freigeben möchten.
2. Ziehen Sie die Datei von ihrem Speicherort in Windows-Explorer auf das Fenster "Freigegebene Dateien" in EasyNetwork.

Tipp: Sie können eine Datei auch freigeben, indem Sie auf **Dateien freigeben** im Menü **Extras** klicken. Navigieren Sie im Dialogfeld "Freigeben" zu dem Ordner, in dem sich die Datei befindet, die freigegeben werden soll, wählen Sie die Datei aus, und klicken Sie auf **Freigeben**.

Freigabe einer Datei aufheben

Wenn Sie eine Datei im verwalteten Netzwerk freigeben, können Sie diese Freigabe jederzeit aufheben. Wenn Sie die Freigabe einer Datei aufheben, können andere Mitglieder des verwalteten Netzwerks nicht mehr darauf zugreifen.

So heben Sie die Freigabe einer Datei auf:

1. Klicken Sie im Menü **Extras** auf **Freigabe von Dateien stoppen**.
2. Wählen Sie im Dialogfeld "Freigabe von Dateien stoppen" die Datei aus, die Sie nicht mehr freigeben möchten.
3. Klicken Sie auf **Nicht freigeben**.

Freigegebene Datei kopieren

Sie können freigegebene Dateien von einem beliebigen Computer im verwalteten Netzwerk auf Ihren Computer kopieren. Wenn der Computer die Dateifreigabe anschließend stoppt, verfügen Sie noch über eine Kopie der Datei.

So kopieren Sie eine Datei:

- Ziehen Sie die Datei aus dem Fenster "Freigegebene Dateien" in EasyNetwork an einen Speicherort in Windows-Explorer oder auf dem Windows-Desktop.

Tipp: Sie können eine freigegebene Datei auch kopieren, indem Sie die Datei in EasyNetwork auswählen und anschließend im Menü **Tools** auf **Kopie an** klicken. Navigieren Sie im Dialogfeld "Kopieren in Ordner" zu dem Ordner, in den Sie die Datei kopieren möchten, wählen Sie die Datei aus und klicken Sie anschließend auf **Speichern**.

Suchen nach einer freigegebenen Datei

Sie können nach einer Datei suchen, die von Ihnen oder einem anderen Mitglied des Netzwerks freigegeben wurde. Während der Eingabe der Suchkriterien zeigt EasyNetwork automatisch die entsprechenden Ergebnisse im Fenster "Freigegebene Dateien" an.

So suchen Sie nach einer freigegebenen Datei:

1. Klicken Sie im Fenster "Freigegebene Dateien" auf **Suche**.
2. Klicken Sie in der Liste **Enthält** auf eine der folgenden Optionen:
   - **Alle Begriffe**: Sucht nach Datei- oder Pfadnamen, die alle Wörter enthalten, die Sie in der Liste **Datei oder Pfadnamen** angeben, in beliebiger Reihenfolge.

- **Ein beliebiger Begriff**: Sucht nach Datei- oder Pfadnamen, die eines der Wörter enthalten, die Sie in der Liste **Datei oder Pfadnamen** angeben.
- **Exakte Zeichenfolge**: Sucht nach Datei- oder Pfadnamen, die den exakten Ausdruck enthalten, den Sie in der Liste **Datei oder Pfadnamen** angeben.

3 Geben Sie einen Teil oder den gesamten Datei- oder Pfadnamen in die Liste **Datei oder Pfadname** ein.

4 Klicken Sie in der Liste **Typ** auf einen der folgenden Dateitypen:

- **Beliebig**: Durchsucht alle freigegebenen Dateitypen.
- **Dokument**: Durchsucht alle freigegebenen Dokumente.
- **Bild**: Durchsucht alle freigegebenen Bilddateien.
- **Video**: Durchsucht alle freigegebenen Videodateien.
- **Audio**: Durchsucht alle freigegebenen Audiodateien.

5 Klicken Sie in den Listen **Von** und **Bis** auf die Daten, die den Datumsbereich festlegen, in dem die Datei erstellt wurde.

Senden von Dateien an andere Computer

Sie können Dateien an andere Computer senden, die Mitglieder des verwalteten Netzwerks sind. Vor dem Senden einer Datei überprüft EasyNetwork, ob der Computer, der die Datei enthält, über ausreichend freien Speicherplatz verfügt.

Wenn Sie eine Datei erhalten, wird diese in Ihrem EasyNetwork-Posteingang angezeigt. Der Posteingang ist ein temporärer Speicherort für alle Dateien, die Sie von anderen Computern im Netzwerk erhalten. Wenn EasyNetwork geöffnet ist, wenn Sie eine Datei erhalten, wird die Datei sofort in Ihrem Posteingang angezeigt; andernfalls wird eine Nachricht im Benachrichtigungsbereich rechts der Windows-Taskleiste angezeigt. Wenn Sie keine Benachrichtigungen erhalten möchten, können Sie diese deaktivieren. Wenn eine Datei mit demselben Namen bereits im Posteingang vorhanden ist, wird dem Namen der neuen Datei eine Zahl als Suffix hinzugefügt. Dateien bleiben in Ihrem Posteingang, bis Sie sie akzeptieren (sie also an einen Speicherort auf Ihrem Computer kopieren).

Eine Datei an einen anderen Computer senden

Sie können eine Datei direkt an einen anderen Computer im verwalteten Netzwerk senden, ohne sie freizugeben. Bevor ein Benutzer die Datei auf dem empfangenden Computer anzeigen kann, muss sie lokal gespeichert werden. Weitere Informationen hierzu finden Sie unter Dateien von einem anderen Computer akzeptieren (Seite 174).

So senden Sie eine Datei an einen anderen Computer:

1. Suchen Sie die zu sendende Datei in Windows-Explorer.
2. Ziehen Sie die Datei in Windows-Explorer von ihrem Speicherort auf ein aktives Computersymbol in EasyNetwork.

Tipp: Sie können mehrere Dateien an einen Computer senden, indem Sie beim Auswählen der Dateien die STRG-Taste gedrückt halten. Sie können die Dateien auch senden, indem Sie im Menü **Tools** auf **Senden** klicken, die Dateien auswählen und anschließend auf **Senden** klicken.

Akzeptieren einer Datei von einem anderen Computer

Wenn ein anderer Computer im verwalteten Netzwerk Ihnen eine Datei sendet, müssen Sie diese akzeptieren (indem Sie sie in einem Ordner auf Ihrem Computer speichern). Wenn EasyNetwork nicht geöffnet ist oder sich nicht im Vordergrund befindet, wenn eine Datei an Ihren Computer gesendet wird, erhalten Sie eine Benachrichtigung im Benachrichtigungsbereich rechts der Taskleiste. Klicken Sie auf die Benachrichtigung, um EasyNetwork zu öffnen und auf die Datei zuzugreifen.

So erhalten Sie eine Datei von einem anderen Computer:

- Klicken Sie auf **Erhalten** und ziehen Sie eine Datei von Ihrem EasyNetwork-Posteingang in einen Ordner in Windows-Explorer.

Tipp: Sie können eine Datei von einem anderen Computer auch erhalten, indem Sie die Datei in Ihrem EasyNetwork-Posteingang auswählen und im Menü **Extras** auf **Akzeptieren** klicken. Navigieren Sie im Dialogfeld "Akzeptieren für Ordner" auf den Ordner, in dem die Dateien, die Sie erhalten, gespeichert werden sollen, wählen Sie ihn aus, und klicken Sie auf **Speichern**.

Benachrichtigung bei gesendeter Datei erhalten

Sie können eine Benachrichtigung erhalten, wenn ein anderer Computer im verwalteten Netzwerk Ihnen eine Datei sendet. Wenn EasyNetwork aktuell nicht geöffnet oder auf dem Desktop nicht im Vordergrund angezeigt wird, wird rechts neben der Windows-Taskleiste eine Benachrichtigungsmeldung angezeigt.

So erhalten Sie Benachrichtungen bei gesendeten Dateien:

1. Kllicken Sie im Menü **Optionen** auf **Konfigurieren**.
2. Aktivieren Sie im Dialogfeld "Konfigurieren" das Kontrollkästchen **Benachrichtigen, wenn Dateien von anderen Computern gesendet werden**.
3. Klicken Sie auf **OK**.

KAPITEL 22

Drucker freigeben

Wenn Sie sich bei einem verwalteten Netzwerk angemeldet haben, gibt EasyNetwork automatisch alle mit Ihrem Computer verbundenen lokalen Drucker frei. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden.

In diesem Kapitel

Mit freigegebenen Druckern arbeiten 176

Mit freigegebenen Druckern arbeiten

Wenn Sie Mitglied eines verwalteten Netzwerks werden, gibt EasyNetwork automatisch alle lokalen Drucker frei, die an Ihren Computer angeschlossen sind. Dabei verwendet es für den Namen der Druckerfreigabe den aktuellen Namen des Druckers. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden. Wenn Sie einen Druckertreiber über einen Netzwerk-Druckerserver konfiguriert haben (z. B. ein Wireless-USB-Druckerserver), betrachtet EasyNetwork den Drucker als lokalen Drucker und gibt ihn automatisch im Netzwerk frei. Sie können eine Druckerfreigabe jederzeit rückgängig machen.

EasyNetwork erkennt auch Drucker, die von allen anderen Computern im Netzwerk freigegeben wurden. Wenn es einen Remote-Drucker erkennt, der noch nicht mit Ihrem Computer verbunden ist, wird beim erstmaligen Öffnen von EasyNetwork im Fenster "Freigegebene Dateien" der Link **Verfügbare Netzwerkdrucker** angezeigt. Dies ermöglicht Ihnen, verfügbare Drucker zu installieren oder Drucker zu deinstallieren, die mit Ihrem Computer bereits verbunden sind. Sie können zudem die Liste der im Netzwerk erkannten Drucker aktualisieren.

Wenn Sie sich beim verwalteten Netzwerk noch nicht angemeldet haben, mit diesem aber bereits verbunden sind, können Sie über die Drucker-Systemsteuerung von Windows auf die freigegebenen Drucker zugreifen.

Freigabe eines Druckers aufheben

Sie können die Freigabe eines Druckers jederzeit aufheben. Mitglieder, die den Drucker installiert haben, können ihn nicht mehr zum Drucken verwenden.

So heben Sie die Freigabe eines Druckers auf:

1. Klicken Sie im Menü **Extras** auf **Drucker**.
2. Klicken Sie im Dialogfeld "Netzwerkdrucker verwalten" auf den Namen des Druckers, den Sie nicht mehr freigeben möchten.
3. Klicken Sie auf **Nicht freigeben**.

Installieren eines verfügbaren Netzwerkdruckers

Als Mitglied eines verwalteten Netzwerks können Sie auf die Drucker zugreifen, die im Netzwerk freigegeben sind. Dazu müssen Sie die Druckertreiber installieren, die der Drucker verwendet. Wenn der Eigentümer des Druckers dessen Freigabe aufhebt, nachdem Sie ihn installiert haben, können Sie mit diesem Drucker nicht mehr drucken.

So installieren Sie einen verfügbaren Netzwerkdrucker:

1. Klicken Sie im Menü **Extras** auf **Drucker**.
2. Klicken Sie im Dialogfeld "Verfügbare Netzwerkdrucker" auf den Namen eines Druckers.
3. Klicken Sie auf **Installieren**.

KAPITEL 23

Referenz

Das Begriffsglossar enthält und definiert die am häufigsten in McAfee-Produkten verwendete Sicherheitsterminologie.

Info zu McAfee enthält rechtliche Informationen zu McAfee Corporation.

Glossar

"

"Man-in-the-Middle"-Angriff

Der Angreifer fängt Nachrichten bei einem öffentlichen Schlüsselaustausch ab und überträgt sie neu, wobei er den angeforderten Schlüssel durch deren eigene öffentliche Schlüssel ersetzt, so dass die beiden ursprünglichen Parteien weiterhin den Eindruck haben, direkt miteinander zu kommunizieren. Dabei verwendet der Angreifer ein Programm, dass sich dem Client gegenüber als Server und dem Server gegenüber als Client ausgibt. Der Angriff kann dazu dienen, einfach nur Zugriff auf die Nachrichten zu erhalten. Der Angreifer hat aber auch die Möglichkeit, die Nachrichten zu ändern, bevor er sie wieder weiterleitet. Der Begriff leitet sich von einem Ballspiel ab, bei dem mehrere Personen versuchen, sich gegenseitig den Ball zuzuwerfen, während ein einzelner Mitspieler in der Mitte versucht, den Ball abzufangen.

8

802.11

Eine Reihe von IEEE-Standards für Funk-LANs. 802.11 legt eine Schnittstelle für den Funkverkehr zwischen einem drahtlosen Client und einer Basisstation oder zwischen zwei drahtlosen Clients fest. Zu den verschiedenen Spezifikationen von 802.11 gehören die Standards 802.11a (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band), 802.11b (für Netzwerke mit einer Bandbreite bis zu 11 Mbit/s im 2,4 GHz-Band), 802.11g (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 2,4 GHz-Band) sowie 802.11i (eine Reihe von Sicherheitsstandards für alle drahtlosen Ethernet-Netzwerke).

802.11a

Eine Erweiterung von 802.11 für Funk-LANs zum Senden von Daten mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band. Dabei ist die Übertragungsgeschwindigkeit zwar größer als bei 802.11b, die Reichweite ist jedoch viel geringer.

802.11b

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 11 Mbit/s im 2,4 GHz-Band bietet. 802.11b gilt derzeit als Standard für drahtlose Netzwerkverbindungen.

802.11g

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 54 Mbit/s im 2,4 GHz-Band bietet.

802.1x

Wird von Wireless Home Network Security nicht unterstützt. Ein IEEE-Standard für die Authentifizierung in kabelgebundenen und drahtlosen Netzwerken, wird aber vor allem in Verbindung mit drahtlosen 802.11-Netzwerken verwendet. Dieser Standard bietet eine starke gegenseitige Authentifizierung zwischen einem Client und einem Authentifizierungsserver. Außerdem bietet 802.1x dynamische, benutzer- und sitzungsspezifische WEP-Schlüssel, wodurch der bei statischen WEP-Schlüsseln übliche Verwaltungsaufwand und die Sicherheitsrisiken beseitigt werden.

A

Anschluss

Hierbei handelt es sich um einen Ort, an dem Informationen bei einem Computer ein- oder ausgehen. Ein konventionelles Analogmodem ist beispielsweise an einen seriellen Anschluss angeschlossen. Die Anschlussnummern bei der TCP/IP-Kommunikation sind virtuelle Werte, die den Datenverkehr in anwendungsspezifische Datenströme aufteilen. Anschlüsse werden Standardprotokollen wie SMTP oder HTTP zugeordnet, damit die Programme "wissen", über welchen Anschluss eine Verbindung hergestellt werden kann. Der Zielanschluss für TCP-Pakete gibt die gesuchte Anwendung oder den gesuchten Server an.

archivieren

Mithilfe dieser Optionen können Sie eine Kopie Ihrer überwachten Dateien lokal auf einem CD-, DVD- oder USB-Laufwerk, einer externen Festplatte oder einem Netzwerk-Laufwerk erstellen.

archivieren

Mithilfe dieser Optionen können Sie eine Kopie Ihrer überwachten Dateien lokal auf einem CD-, DVD- oder USB-Laufwerk, einer externen Festplatte oder einem Netzwerk-Laufwerk erstellen.

Authentifizierung

Der Vorgang des Identifizierens eines bestimmten Benutzers, meist anhand von Benutzername und Kennwort. Mit der Authentifizierung wird sichergestellt, dass es sich bei einem Benutzer auch wirklich um denjenigen handelt, der er oder sie zu sein vorgibt. Über die Zugriffsrechte dieses Benutzers sagt die Authentifizierung jedoch nichts aus.

B

Bandbreite

Die Datenmenge, die innerhalb eines bestimmten Zeitraums übertragen werden kann. Bei digitalen Geräten wird die Bandbreite meist in Bit pro Sekunde (Bit/s) oder Byte pro Sekunde angegeben. Bei analogen Geräten wird die Bandbreite als Taktzahl pro Sekunde bzw. Hertz (Hz) angegeben.

Bibliothek

Der Online-Speicherbereich für Dateien, die von Benutzern der Datensicherung veröffentlicht werden. Die Bibliothekt ist eine Website im Internet, auf die jeder mit Internetzugriff zugreifen kann.

Bilderanalyse

Verhindert die Anzeige potentiell unangemessener Bilder. Bilder werden für alle Benutzer blockiert, außer für Mitglieder der Altersgruppe "Erwachsener".

Browser

Ein Clientprogramm, das mit Hilfe von HTTP (Hypertext Transfer Protocol) Anforderungen an Webserver im Internet richtet. Ein Webbrowser zeigt dem Benutzer den Inhalt graphisch an.

Brute-Force-Angriff

Eine Vorgehensweise nach dem Fehler-Treffer-Prinzip, die auch unter dem Begriff "Brute-Force-Cracking" bekannt ist. Dabei versuchen entsprechende Programme, verschlüsselte Daten (z. B. Kennwörter) mithilfe eines riesigen Aufwands (mit "purer Gewalt") anstatt durch zielgerichtete Strategien zu entschlüsseln.
Brute-Force-Anwendungen probieren nacheinander alle möglichen Kombinationen von zulässigen Zeichen aus – wie bei einem Safe, bei dem alle Zahlenkombinationen ausprobiert werden, um ihn zu öffnen, was genauso eine strafbare Handlung ist.
Brute-Force-Angriffe werden als eine Methode betrachtet, die, wenn auch mit großen Zeitaufwand verbunden, irgendwann schließlich zum Erfolg führt.

C

chiffrierter Text

Das sind Daten, die verschlüsselt wurden. Chiffrierter Text ist nicht lesbar, solange er nicht mithilfe eines Schlüssels wieder in Klartext umgewandelt (entschlüsselt) wurde.

Client

Eine Anwendung, die auf einem PC oder einer Workstation ausgeführt wird und zum Durchführen bestimmter Vorgänge auf einen Server angewiesen ist. Beispiel: Ein E-Mail-Client ist eine Anwendung, mit der Sie E-Mails senden und empfangen können.

Cookie

Ein Datenblock im World Wide Web, den ein Webserver auf einem Clientsystem speichert. Wenn ein Benutzer erneut dieselbe Website besucht, sendet der Browser eine Kopie des Cookies zurück an den Server. Cookies werden für die Identifizierung von Benutzern, zur Anweisung an den Server, eine benutzerdefinierte Version der angeforderten Webseite zu senden, zum Senden von Kontoinformationen an den Benutzer sowie für andere administrative Aufgaben verwendet.

Diese Datei ermöglicht es, dass die Website sich an Sie "erinnert", und der Betreiber kann feststellen, wie viele Benutzer die Website besucht haben bzw. wann welche Seiten der Website aufgerufen wurden. Unternehmen versuchen, ihre Websites mithilfe von Cookies gezielt auf die Vorlieben und Anforderungen verschiedener Benutzer abzustimmen. Zahlreiche Websites gestatten beispielsweise den Zugriff auf bestimmte Seiten der Website erst dann, wenn Sie einen Benutzernamen und ein Kennwort eingeben, und senden ein Cookie an Ihren Computer, so dass Sie sich beim nächsten Besuch dieser Seiten nicht erneut anmelden müssen. Cookies können jedoch auch missbraucht werden. Online-Werbefirmen verwenden oft Cookies, um zu analysieren, welche Websites häufig von Ihnen besucht werden, und nutzen diese Erkenntnisse zum Platzieren von Werbeanzeigen auf den meistbesuchten Websites. Bevor Sie Cookies von einer Website zulassen, sollten Sie sicher sein, dass Sie dieser Website vertrauen können.

Cookies sind nicht nur für rechtsgültige Unternehmen eine Informationsquelle, sondern können zu diesem Zweck auch von Hackern missbraucht werden. Zahlreiche Websites von Onlineshops speichern Kreditkartennummern und andere persönliche Informationen in Cookies, um den Kunden das Einkaufen zu erleichtern. Leider sind Sicherheitslücken nicht auszuschließen, die es Hackern ermöglichen, über die auf den Kundencomputern gespeicherten Cookies auf vertrauliche Daten zuzugreifen.

D

Denial of Service, DoS

Ein DoS-Angriff (Denial-of-Service, Dienstverweigerung) ist ein Störfall im Internet, durch den Benutzer oder Unternehmen nicht mehr auf bestimmte Ressourcen oder Dienste zugreifen können. Dabei handelt es sich meist um die Nichtverfügbarkeit eines einzelnen Netzwerkdienstes (z. B. E-Mail) oder den vorübergehenden Verlust aller Netzwerkverbindungen und -dienste. Im schlimmsten Fall kann beispielsweise eine Website, auf die täglich Millionen Benutzer zugreifen, zeitweise gezwungen sein, ihren Betrieb einzustellen. Bei einem DoS-Angriff können auch Programme und Dateien in einem Computersystem zerstört werden. Auch wenn DoS-Angriffe meist absichtlich und böswillig sind, können sie manchmal auch unbeabsichtigt passieren. Ein DoS-Angriff stellt eine Art von Sicherheitsverletzung dar, die meist nicht zu einem Diebstahl von Informationen oder anderen Sicherheitsverlusten führt. Trotzdem können solche Angriffe für die Zielperson bzw. das geschädigte Unternehmen mit einem beträchtlichen Zeitaufwand und erheblichen Kosten verbunden sein.

DNS

Acronym für Domain Name System. Das hierarchische System, über das Hosts im Internet sowohl Domänennamenadressen (wie bluestem.prairienet.org) und IP-Adressen (wie 192.17.3.4) erhalten. Die Domänennamenadresse wird von Personen verwendet und automatisch in die numerische IP-Adresse übersetzt, die von der Paket-Weiterleitungssoftware verwendet wird. DNS-Namen bestehen aus einer Domäne auf der obersten Ebene (wie .com, .org, und .net), einer Domäne auf der zweiten Ebene (der Site-Name eines Unternehmens, einer Organisation oder einer Einzelperson) und möglicherweise einer oder mehreren untergeordneten Domänen (Server innerhalb einer Domäne auf der zweiten Ebene). Siehe auch DNS-Server und IP-Adresse.

DNS-Server

Abkürzung für Domain Name System-Server. Ein Computer, der Domain Name System (DNS)-Abfragen beantworten kann. Der DNS-Server verwaltet eine Datenbank mit Host-Computern und ihren dazugehörigen IP-Adressen. Der DNS-Server, der durch den Namen apex.com dargestellt wird, würde beispielsweise die IP-Adresse des fiktiven Unternehmens Apex zurückgeben. Auch bezeichnet als: Namensserver Siehe auch DNS- und IP-Adresse.

Domäne

Eine Adresse einer Netzwerkverbindung, die den Inhaber dieser Adresse in einem hierarchischen Format identifiziert: server.organisation.typ. Beispielsweise bezeichnet www.whitehouse.gov den Webserver des Weißen Hauses, das Teil der US-Regierung ist.

Drahtloser Adapter

Enthält die Schaltkreise, mit denen ein Computer oder ein anderes Gerät mit einem (an einem drahtlosen Netzwerk angeschlossenen) drahtlosen Router kommunizieren kann. Drahtlose Adapter können entweder im Hauptschaltkreis eines Hardwaregeräts integriert sein oder sich auf einer separaten Zusatzkarte befinden, die in den entsprechenden Anschluss eines Geräts eingesteckt wird.

E

E-Mail

E-Mails sind "elektronische Post", also Nachrichten, die über das Internet oder innerhalb eines Unternehmens über LAN oder WAN gesendet werden. E-Mail-Anlagen in Form von EXE-Dateien (ausführbare Dateien) oder VBS-Dateien (Visual Basic-Skriptdateien) werden immer häufiger für die Übertragung von Viren und trojanischen Pferden zweckentfremdet.

E-Mail-Client

Ein E-Mail-Konto. Beispielsweise Microsoft Outlook oder Eudora.

Echtzeit-Scans

Dateien werden auf Viren und andere Aktivitäten gescannt, wenn Sie oder Ihr Computer darauf zugreifen.

Ereignis

Ereignisse von 0.0.0.0

Wenn Ereignisse mit der IP-Adresse 0.0.0.0 angezeigt werden, gibt es hierfür zwei mögliche Ursachen. Die erste und häufigste Ursache ist die, dass Ihr Computer ein fehlerhaftes Paket erhalten hat. Das Internet ist nicht zu 100 % zuverlässig, und es ist immer möglich, dass fehlerhafte Pakete eingehen. Da Firewall die Pakete vor der TCP/IP-Validierung erhält, kann es solche Pakete möglicherweise als Ereignis melden.

Die zweite Ursache ist die, dass die Quell-IP-Adresse gefälscht wurde. Gefälschte Pakete sind möglicherweise ein Anzeichen dafür, dass jemand auf Ihrem Computer nach einem Trojaner gesucht hat. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert.

Ereignisse von 127.0.0.1

Manchmal wird von Ereignissen als IP-Quelladresse 127.0.0.1 angegeben. Hierbei ist zu beachten, dass es sich um eine spezielle IP-Adresse handelt, die auch Loopbackadresse genannt wird.

Unabhängig davon, welchen Computer Sie verwenden, 127.0.0.1 bezieht sich stets auf Ihren lokalen Computer. Diese Adresse wird auch Localhost genannt, weil der Computername "Localhost" immer die IP-Adresse 127.0.0.1 auflöst. Bedeutet dies, dass der Computer einen Angriff auf sich selbst ausübt? Wird Ihr Computer von einem trojanischen Pferd oder von Spyware angegriffen? Dies ist sehr unwahrscheinlich. Viele seriöse Programme verwenden die Loopbackadresse zur Kommunikation zwischen den Komponenten. Zahlreiche persönliche E-Mail- oder Webserver lassen sich beispielsweise über eine Weboberfläche konfigurieren, auf die über die Adresse "http://localhost/" (oder eine vergleichbare Adresse) zugegriffen werden kann.

Firewall lässt Datenverkehr von diesen Programmen zu. Wenn Ereignisse mit der IP-Adresse 127.0.0.1 angezeigt werden, bedeutet dies in der Regel, dass die Quell-IP-Adresse gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach trojanischen Pferden sucht. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert. Das Erstellen von Berichten zu Ereignissen der IP-Adresse 127.0.0.1 ist offensichtlich nicht hilfreich und daher unnötig.

Das heißt, dass für einige Programme, vor allem Netscape ab Version 6.2 und höher gilt, jedoch dass die Adresse 127.0.0.1 in die Liste **Vertrauenswürdige IP-Adressen** aufgenommen werden muss. Die Komponenten dieser Programme kommunizieren so miteinander, dass Firewall nicht bestimmen kann, ob es sich um einen lokalen Datenverkehr handelt oder nicht.

Bei Netscape 6.2 können Sie zum Beispiel Ihre Buddyliste nicht verwenden, wenn Sie die Adresse 127.0.0.1 nicht als vertrauenswürdig einstufen. Wenn Sie also Datenverkehr von 127.0.0.1 bemerken und alle Anwendungen auf Ihrem Computer normal funktionieren, können Sie diesen Datenverkehr sicherheitshalber blockieren. Sollte jedoch ein Programm (wie Netscape) Probleme haben, nehmen Sie die Adresse 127.0.0.1 in die Liste **Vertrauenswürdige IP-Adressen** in Firewall auf, und ermitteln Sie anschließend, ob das Problem behoben ist.

Wird das Problem durch die Aufnahme von 127.0.0.1 in die Liste **Vertrauenswürdige IP-Adressen** behoben, müssen Sie Ihre Entscheidungsmöglichkeiten abwägen: Wenn Sie die Adresse 127.0.0.1 als vertrauenswürdig einstufen, funktioniert zwar das Programm, allerdings erhöht sich die Gefahr, dass Angriffe mit gefälschten Adressen ausgeführt werden. Wenn Sie diese Adresse nicht als vertrauenswürdig einstufen, funktioniert das Programm nicht. Es wird in diesem Fall jedoch die Gefahr verringert, dass Angriffe mit gefälschten Adressen ausgeführt werden.

Ereignisse von Computern in Ihrem LAN

Für die meisten LAN-Einstellungen in Unternehmen können Sie allen Computern in Ihrem LAN vertrauen.

Ereignisse von privaten IP-Adressen

IP-Adressen im Format 192.168.xxx.xxx, 10.xxx.xxx.xxx und 172.16.0.0 bis 172.31.255.255 werden als nicht routbare oder private IP-Adressen bezeichnet. Diese IP-Adressen sollten Ihr Netzwerk nie verlassen und können in der Regel als vertrauenswürdig angesehen werden.

Der Block 192.168 wird in Zusammenhang mit Microsoft Internet Connection Sharing (ICS) verwendet. Wenn Sie ICS verwenden und Ereignisse von diesem IP-Block angezeigt werden, können Sie die IP-Adresse 192.168.255.255 in die Liste **Vertrauenswürdige IP-Adressen** aufnehmen. Dadurch wird der Block 192.168.xxx.xxx als vertrauenswürdig eingestuft.

Wenn Sie sich nicht in einem privaten Netzwerk befinden und Ereignisse von diesen IP-Bereichen angezeigt werden, bedeutet dies, dass die IP-Quelladresse möglicherweise gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach trojanischen Pferden sucht. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert.

Da private IP-Adressen von IP-Adressen im Internet getrennt sind, hat das Melden dieser Ereignisse keine Auswirkungen.

ESS (Extended Service Set)

Eine Gruppe von mindestens zwei Netzwerken, die ein Subnetz bilden.

Externe Festplatte

Eine Festplatte, die außerhalb des Computergehäuses aufbewahrt wird.

Firewall

Ein System, das dazu dient, nicht autorisierte Zugriffe auf ein bzw. aus einem privaten Netzwerk zu verhindern. Firewalls können in Form von Hardware, Software oder einer Kombination von beiden implementiert werden. Sie werden häufig verwendet, um zu verhindern, dass nicht autorisierte Internetbenutzer auf private Netzwerke (insbesondere Intranets) zugreifen, die mit dem Internet verbunden sind. Alle Nachrichten, die in das Intranet gelangen oder dieses verlassen, laufen durch eine Firewall. Von dieser werden alle Nachrichten überprüft und jene blockiert, die nicht die angegebenen Sicherheitskriterien erfüllen. Firewalls werden als erste Verteidigungslinie beim Schutz privater Informationen betrachtet. Zur höheren Sicherheit können die Daten verschlüsselt werden.

Freigeben

Ein Vorgang, der es E-Mail-Empfängern ermöglicht, für eine begrenzte Zeit auf ausgewählte gesicherte Dateien zuzugreifen. Wenn Sie eine Datei freigeben, senden Sie die gesicherte Kopie der Datei an die E-Mail-Empfänger, die Sie angeben. Die Empfänger erhalten eine E-Mail der Datensicherung, die ihnen mitteilt, dass Dateien für sie freigegeben wurden. Die E-Mail enthält außerdem einen Link zu den freigegebenen Dateien.

freigegebenes Geheimnis

Siehe auch RADIUS. Schützt den sensiblen Teil von RADIUS-Nachrichten. Der gemeinsame geheime Schlüssel ist ein Kennwort, das von dem Authentifikator und dem Authentifizierungsserver auf eine bestimmte sichere Weise gemeinsam verwendet wird.

Hotspot

Ein bestimmter örtlicher Standort, an dem ein Zugriffspunkt mobilen Besuchern den Zugriff auf öffentliche Breitband-Netzwerkdienste über ein drahtloses Netzwerk ermöglicht. Hotspots befinden sich oft in der Nähe von stark frequentierten Einrichtungen, z. B. Flughäfen, Bahnhöfen, Bibliotheken, Jachthäfen, Messe-Centern und Hotels. Sie haben meist eine geringe Reichweite.

Inhaltsklassifikationsgruppen

Altersgruppen, zu denen ein Benutzer gehört. Der Inhalt wird auf der Grundlage der Inhaltsklassifikationsgruppe bewertet (das bedeutet verfügbar gemacht oder blockiert), zu der der Benutzer gehört. Inhaltsklassifikationsgruppen umfassen Folgendes: kleines Kind, Kind, jüngerer Teenager, älterer Teenager und Erwachsener.

integriertes Gateway

Ein Gerät, in dem die Funktionen eines Zugriffspunkts, Routers und einer Firewall kombiniert sind. Einige Geräte können auch Sicherheitsoptimierungen und Überbrückungsfunktionen enthalten.

Internet

Das Internet besteht aus einer großen Menge verbundener Netzwerke, die TCP/IP-Protokolle zur Ermittlung und Übertragung von Daten verwenden. Ursprünglich ist das Internet aus miteinander verbundenen Universitätscomputern entstanden. Daraus entwickelte sich das Ende der 60er Jahre vom US-Verteidigungsministerium gegründete ARPANET, das als Wegbereiter für das Internet gilt. Heute ist das Internet ein globales Netzwerk von nahezu 100.000 unabhängigen Netzwerken.

Intranet

Ein privates Netzwerk, in der Regel innerhalb einer Organisation, das im Wesentlichen wie das Internet funktioniert. Auf ein Intranet kann auch von externen Computern aus zugegriffen werden, beispielsweise durch Studenten, die auf das Intranet einer Universität, oder externe Mitarbeiter, die auf das Internet eines Unternehmens Zugriff erhalten haben. Firewalls, Anmeldeprozeduren und Kennwörter dienen der Sicherheit eines Intranets.

IP-Adresse

Die IP-Adresse (Internet Protocol Number) ist eine eindeutige Zahlenfolge, deren vier Bestandteile durch Punkte voneinander getrennt sind (z. B. 63.227.89.66). Jeder Internetcomputer verfügt über eine eindeutige IP-Adresse - vom größten Server bis hin zum Laptop, der per Mobilanschluss kommuniziert. Nicht jeder Computer weist einen Domänennamen auf, aber jeder Computer hat eine IP-Adresse.

Im Folgenden werden einige ungewöhnliche Typen von IP-Adressen aufgeführt:

- Nicht routbare IP-Adressen: Diese stellen einen privaten IP-Adressraum dar. Hierbei handelt es sich um IP-Adressen, die im Internet nicht verwendet werden können. Private IP-Blöcke sind 10.x.x.x, 172.16.x.x bis 172.31.x.x und 192.168.x.x.
- Loopback-IP-Adressen**:** Diese Adressen werden zu Testzwecken verwendet. Datenpakete, die an diesen IP-Adressblock gesendet werden, kehren sofort wieder zu dem Gerät zurück, von dem das Paket generiert wurde. Da an diese IP-Adressen gerichtete Datenpakete das Gerät überhaupt nicht verlassen, werden diese Adressen hauptsächlich für Hardware- und Softwaretests verwendet. Der Loopback-IP-Block beginnt mit 127.x.x.x.

Null-IP-Adressen Hierbei handelt es sich um eine ungültige Adresse. Eine Null-IP-Adresse weist darauf hin, dass im Datenverkehr eine leere IP-Adresse verwendet wurde und der Absender den Ursprung des Datenverkehrs nicht preisgeben möchte. Der Absender kann keine Antwort auf den Datenverkehr erhalten, es sei denn, das Paket wird von einer Anwendung empfangen, die den Paketinhalt (d. h. die anwendungsspezifischen Anweisungen) versteht und damit entsprechend umgehen kann. Jede Adresse, die mit 0 beginnt (0.x.x.x), ist eine Null-Adresse. Beispiel: 0.0.0.0 ist eine Null-IP-Adresse.

IP-Spoofing

Das Fälschen der IP-Adressen in einem IP-Paket. Dieses Methode wird in vielen Arten von Angriffen einschließlich dem "Session-Hijacking" verwendet. Sie wird oftmals auch dazu verwendet, die Kopfzeilen von SPAM-E-Mails zu fälschen, damit diese E-Mails nicht mehr zurückverfolgt werden können.

isolieren

Wenn verdächtige Dateien erkannt werden, werden sie isoliert. Sie können dann die entsprechende Aktion ausführen.

Kennwort

Ein (in der Regel alphanumerischer) Code, über den Sie Zugriff auf Ihren Computer bzw. auf ein Programm oder eine Website erhalten.

Kennwort-Tresor

Ein sicherer Speicherbereich für Ihre persönlichen Kennwörter. Er ermöglicht es Ihnen, Ihre Kennwörter sicher zu speichern in dem Wissen, dass kein anderer Benutzer (auch kein McAfee-Administrator oder Systemadministrator) darauf zugreifen kann.

Knoten

Hierbei handelt es sich um einen Computer, der mit einem Netzwerk verbunden ist.

Komprimierung

Ein Vorgang, bei dem Daten (Dateien) in eine Form komprimiert werden, die den zum Speichern oder Übermitteln erforderlichen Platz minimiert.

Kopfzeile

Bei einem Header handelt es sich um Informationen, die im Lauf der Übermittlung zur E-Mail hinzugefügt wurden. Die Kopfzeile bestimmt die Übermittlung der E-Mail durch die Internetsoftware und enthält außerdem die Adresse für die Rückantwort, eine eindeutige Kennung für die E-Mail und andere administrative Angaben. Beispiele für diese Kopfzeilenfelder sind: An, Von, CC, Datum, Betreff, Nachrichten-ID und Empfangen.

LAN (Local Area Network)

Ein Computernetzwerk, dass sich über ein relativ kleines Gebiet erstreckt. Die meisten LANs sind auf ein einzelnes Gebäude oder eine Gruppe von Gebäuden beschränkt. Per Telefonverbindungen oder Funkwellen kann ein LAN aber auch über eine beliebige Entfernung mit anderen LANs verbunden werden. Ein System aus LANs, die auf diese Weise miteinander verbunden sind, wird WAN (Wide-Area Network) genannt. In den meisten LANs werden Workstations und PCs über normale Hubs oder Switches miteinander verbunden. Jeder Knoten (ein einzelner Computer) in einem LAN hat seine eigene CPU, mit der er Programme ausführt, kann aber auch auf Daten und Geräte (z. B. Drucker) im LAN zugreifen. Auf diese Weise können teure Geräte (z. B. Laserdrucker) sowie Daten von vielen Benutzern gemeinsam genutzt werden. Über ein LAN können Benutzer auch miteinander kommunizieren, z. B. E-Mails senden oder an Chat-Sitzungen teilnehmen.

MAC (Media Access Control oder Message Authenticator Code)

Für das Erstgenannte von beiden siehe "MAC-Adresse". Die zweite ausgeschriebene Abkürzung (Message Authenticator Code) bezeichnet einen Code, der zum Identifizieren einer bestimmten Nachricht (z. B. einer RADIUS-Nachricht) verwendet wird. Der Code ist gewöhnlich ein kryptographisch starker Hash des Nachrichteninhalts, der einen eindeutigen Wert als Replay-Schutz enthält.

MAC-Adresse (Media Access Control Address)

Eine Adresse auf unterer Ebene, die einem physikalischen Gerät zugewiesen wird, das auf das Netzwerk zugreift.

MAPI-Konto

Acronym für Messaging Application Programming Interface. Die Microsoft-Schnittstellenspezifikation, die es verschiedenen Messaging- und Arbeitsgruppenanwendungen (einschließlich E-Mail, Voice-Mail und Fax) ermöglicht, einen einzigen Client zu verwenden, wie den Exchange-Client. MAPI wird daher häufig in Unternehmensumgebungen mit Microsoft® Exchange Server eingesetzt. Zahlreiche Benutzer verwenden allerdings Microsoft Outlook für persönliche Internet-E-Mails.

MSN-Konto

Acronym für Microsoft Network. Ein Online-Dienst und Internetportal. Dies ist ein webbasiertes Konto.

Netzwerk

Ein Netzwerk entsteht durch die Verbindung von mehreren Computern.

Netzwerk-Laufwerk

Ein Disketten- oder Band-Laufwerk, das mit einem Server in einem Netzwerk verbunden ist, das für mehrere Benutzer freigegeben ist. Netzwerk-Laufwerke werden gelegentlich auch als Remote-Laufwerke bezeichnet.

Netzwerkzuordnung

In Network Manager ist die Netzwerkzuordnung eine graphische Darstellung des Computers und der Komponenten, die Ihr privates Netzwerk ausmachen.

NIC (Network Interface Card, Netzwerkkarte)

Eine Karte, die in ein Notebook oder ein anderes Gerät gesteckt wird und das Gerät mit dem LAN verbindet.

Online-Sicherungs-Repository

Der Speicherort auf dem Online-Server, an dem Ihre überwachten Dateien nach der Sicherung gespeichert werden.

Parental controls

Einstellungen, die das Konfigurieren von Inhaltsklassifikationen und Internetzugriffszeiten ermöglichen. Darin wird festgelegt, welche Inhalte und Websites ein Benutzer anzeigen kann und wann und wie lange dieser Benutzer auf das Internet zugreifen kann. Mit Kindersicherungen können Sie außerdem allgemeine Beschränkungen für den Zugriff auf bestimmte Websites festlegen oder den Zugriff auf der Grundlage von Altersgruppen und Stichwörtern gewähren oder blockieren.

PCI-Drahtlosadapter-Karte

Verbindet einen Desktopcomputer mit einem Netzwerk. Die Karte wird in einen PCI-Erweiterungssteckplatz im Computer gesteckt.

Phishing

Als "Fishing" ausgesprochen, ist ein Scam, mithilfe dessen Ihnen wertvolle Informationen, wie Ihre Kreditkarten- und Sozialversicherungsnummer, Benutzer-IDs und Kennwörter gestohlen werden sollen. Eine offiziell aussehende E-Mail wird an potentielle Opfer gesendet. Dabei wird behauptet, die Mail stamme vom ISP, der Bank oder einem Geschäft, bei dem die Benutzer einkaufen. E-Mails können an Personen auf ausgewählten oder beliebigen Listen gesendet werden, in der Erwartung, dass ein gewisser Prozentsatz der Empfänger tatsächlich über ein Konto bei dem echten Unternehmen verfügt.

POP3-Konto

Acronym für Post Office Protocol 3. Die meisten privaten Benutzer haben diesen Kontotyp. Dies ist die aktuelle Version des Post Office Protocol-Standards, der häufig in TCP/IP-Netzwerken verwendet wird. Auch bekannt als standardmäßiges E-Mail-Konto.

Popups

Kleine Fenster, die über anderen Fenstern auf dem Bildschirm angezeigt werden. Popup-Fenster werden oft in Webbrowsern verwendet, um Werbung anzuzeigen. McAfee blockiert Popup-Fenster, die automatisch geladen werden, wenn eine Webseite in Ihrem Browser geladen wird. Popup-Fenster, die geladen werden, wenn Sie auf einen Link klicken, werden von McAfee nicht blockiert.

Potentiell unerwünschtes Programm

Potentiell unerwünschte Programme umfassen Spyware, Adware und andere Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und übertragen.

PPPoE

Abkürzung für "Point-to-Point Protocol Over Ethernet". PPPoE wird von vielen DSL-Providern verwendet und unterstützt die in PPP häufig verwendeten Protokollebenen und Authentifizierung. Mit PPPoE kann eine Punkt-zu-Punkt-Verbindung in der normalen Multipoint-Ethernet-Architektur hergestellt werden.

Protokoll

Ein vorab vereinbartes Format zum Übertragen von Daten zwischen zwei Geräten. Aus Sicht des Benutzers besteht der einzige interessante Aspekt bei Protokollen darin, dass der Computer oder das Gerät die entsprechenden Protokolle unterstützen muss, um mit einem jeweils anderen Computer kommunizieren zu können. Das Protokoll kann entweder in der Hardware oder in der Software implementiert sein.

Proxy

Ein Computer (oder die auf ihm ausgeführte Software), der als Barriere zwischen einem Netzwerk und dem Internet fungiert, indem er gegenüber externen Sites nur als eine einzige Netzwerkadresse auftritt. Indem er für alle internen Computer eine Zwischenwand darstellt, schützt der Proxy Netzwerkidentitäten und ermöglicht gleichzeitig Zugriff auf das Internet. Siehe auch Proxyserver.

Proxy-Server

Eine Firewallkomponente, die den ein- und ausgehenden Internetverkehr eines LAN (Local Area Network) verwaltet. Ein Proxyserver kann durch Liefern häufig angeforderter Daten, z.B. einer beliebten Webseite, die Leistung steigern und Anforderungen filtern, die der Eigentümer als nicht geeignet einstuft, z.B. Anforderungen nach unautorisiertem Zugriff auf proprietäre Dateien.

Pufferüberlauf

Pufferüberläufe finden statt, wenn verdächtige Programme oder Prozesse versuchen, mehr Daten in einem Puffer (Speicherbereich für temporäre Dateien) auf Ihrem Computer zu speichern als erlaubt, so dass gültige Daten in nahegelegenen Puffern beschädigt oder überschrieben würden.

RADIUS (Remote Access Dial-In User Service)

Ein Protokoll zum Authentifizieren von Benutzern, meist im Zusammenhang mit Remote-Zugriff. Ursprünglich definiert für den Einsatz in RAS-Einwahl-Servern, wird das Protokoll heutzutage in einer breiten Vielzahl von Authentifizierungsumgebungen genutzt, einschließlich der 802.1x-Authentifizierung des gemeinsamen geheimen Schlüssels von WLAN-Benutzern.

Reiner Text

Nachrichten, die nicht verschlüsselt sind.

Roaming

Die Fähigkeit, aus dem Empfangsbereich eines Zugriffspunkts in den eines anderen zu wechseln, ohne dass dabei der Betrieb unterbrochen oder die Verbindung verloren wird.

Router

Ein Netzwerkgerät, das Pakete von einem Netzwerk in ein anderes weiterleitet. Router lesen jedes eingehende Paket und entscheiden anhand interner Routingtabellen, wie das Paket weitergeleitet werden soll. Die Wahl der Schnittstelle, an die ausgehende Pakete gesendet werden, kann davon abhängen, in welcher Konstellation Quell- und Zieladresse miteinander stehen, oder sich nach den aktuellen Gegebenheiten im Netzwerkverkehr (z. B. Auslastung, Leitungskosten oder ausgefallene Leitungen) richten. Für "Router" wird manchmal auch der Begriff "Zugriffspunkt" verwendet.

Schlüssel

Eine Folge von Buchstaben und/oder Zahlen, mit der zwei Geräte ihre Kommunikation miteinander authentifizieren können. Dabei müssen beide Geräte über den Schlüssel verfügen. Siehe auch WEP, WPA, WPA2, WPA-PSK und WPA2- PSK.

Schnellarchivierung

Die Archivierung nur der überwachten Dateien, die seit der letzten vollständigen Archivierung oder Schnellarchivierung geändert wurden.

Schwarze Liste

Eine Liste der Websites, die als schädlich angesehen werden. Eine Website kann in eine schwarze Liste eingetragen werden, wenn über sie betrügerische Handlungen vorgenommen werden oder wenn sie Browser-Schwachstellen ausnutzt, um potentiell unerwünschte Programme an den Benutzer zu senden.

Server

Hierbei handelt es sich um einen Computer oder eine Software, der/die bestimmte Dienste für das Ausführen einer Software auf anderen Computern zur Verfügung stellt. Der "E-Mail-Server" bei Ihrem ISP ist eine Software, die den gesamten eingehenden und ausgehenden E-Mail-Datenverkehr für alle Benutzer des ISPs verarbeitet. Bei einem Server auf einem LAN handelt es sich um eine Hardware, die den primären Knoten im Netzwerk darstellt. Diese Hardware kann wiederum Software enthalten, die den zugehörigen Clientcomputern bestimmte Dienste, Daten oder andere Funktionen zur Verfügung stellt.

sichern

Verwenden Sie diese Option, um eine Kopie Ihrer überwachten Dateien auf einem sicheren Online-Server zu erstellen.

Skript

Skripts können Dateien erstellen, kopieren oder löschen. Sie können auch Ihre Windows-Registrierung öffnen.

SMTP-Server

Acronym für Simple Mail Transfer Protocol. Ein TCP/IP-Protokoll, das für das Senden von Nachrichten von einem Computer an einen anderen in einem Netzwerk verwendet wird. Dieses Protokoll wird im Internet verwendet, um E-Mails weiterzuleiten.

Speicherort für die oberflächliche Überwachung

Ein Ordner auf Ihrem Computer, der von der Datensicherung auf Änderungen überwacht wird. Wenn Sie einen Speicherort für die oberflächliche Überwachung einrichten, sichert die Datensicherung die überwachten Dateitypen innerhalb dieses Ordners, nicht aber innerhalb der Unterordner.

Speicherort für umfassende Überwachung

Ein Ordner (und alle Unterordner) auf Ihrem Computer, der von Data Backup auf Änderungen hin überwacht wird. Wenn Sie einen Speicherort für die umfassende Überwachung festlegen, sichert Data Backup die überwachten Dateitypen in diesem Order und seinen Unterordnern.

SSID (Service Set Identifier)

Der Netzwerkname für die Geräte in einem Funk-LAN-Subsystem. Das ist eine Zeichenfolge aus 32 Zeichen, die im Klartext steht und zum Kopf jedes WLAN-Pakets hinzugefügt wird. Die SSID unterscheidet WLANs voneinander. Daher müssen alle Benutzer eines Netzwerks dieselbe SSID angeben, um auf einen bestimmten Zugriffspunkt zuzugreifen. Mit einer SSID wird der Zugriff von Clientgeräten verhindert, die eine andere SSID besitzen. Die SSID wird jedoch von Zugriffspunkten standardmäßig zusammen mit dem Signal übertragen. Dadurch kann ein Hacker die SSID per "Sniffing" selbst dann ermitteln, wenn die SSID-Übertragung deaktiviert ist.

SSL (Secure Sockets Layer)

Ein von Netscape entwickeltes Protokoll zum Übermitteln vertraulicher Dokumente über das Internet. SSL arbeitet mit einem öffentlichen Schlüssel, mit dem die Daten verschlüsselt werden, die über die SSL-Verbindung übertragen werden. SSL wird sowohl von Netscape Navigator als auch von Internet Explorer genutzt und unterstützt. Viele Websites verwenden dieses Protokoll, wenn Benutzer vertrauliche Informationen (z. B. Kreditkartennummern) eingeben müssen. Laut Konvention beginnen URLs, die eine SSL-Verbindung erfordern, mit der Zeichenfolge "https:" anstelle von "http:".

Standard-E-Mail-Konto

Dies ist die am häufigsten vorkommende Kontoart. Siehe auch POP3-Konto.

Stichwort

Ein Wort, das Sie einer gesicherten Datei zuordnen können, um eine Beziehung oder Verbindung mit anderen Dateien aufzubauen, denen dasselbe Stichwort zugeordnet ist. Durch das Zuordnen von Stichwörtern zu Dateien ist es einfacher, nach Dateien zu suchen, die Sie im Internet veröffentlicht haben.

Synchronisieren

Zur Behebung von Inkonsistenzen zwischen gesicherten Dateien und den auf Ihrem lokalen Computer gespeicherten Dateien. Sie synchronisieren Dateien, wenn die Version der Datei im Online-Sicherungs-Repository aktueller als die Version der Datei auf den anderen Computern ist. Durch die Synchronisierung wird die Kopie der Datei auf Ihren Computern mit der Version der Datei im Online-Sicherungs-Repository aktualisiert.

SystemGuard

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus.

TKIP (Temporal Key Integrity Protocol)

Eine schnelle Methode zum Lösen der konstruktionsbedingten Sicherheitsschwächen von WEP, speziell des Problems der Wiederverwendung von Verschlüsselungsschlüsseln. Bei TKIP werden temporäre Schlüssel nach jeweils 10.000 Paketen geändert. Auf diese Weise wird eine dynamische Verteilungsmethode erzielt, die die Sicherheit des Netzwerks beträchtlich erhöht. Der TKIP-Sicherheitsprozess beginnt mit einem temporären 128-Bit-Schlüssel, der von Clients und Zugriffspunkten gemeinsam verwendet wird. TKIP kombiniert diesen temporären Schlüssel mit der MAC-Adresse (des Clientcomputers) und fügt dann einen relativ großen Initialisierungsvektor (16 Oktetts) hinzu, um den Schlüssel zu erstellen, mit dem die Daten verschlüsselt werden. Durch diese Vorgehensweise wird sichergestellt, dass jede Station ihre Daten mit einem anderen Schlüssel-Stream verschlüsselt. TKIP führt die Verschlüsselung mit RC4 durch. WEP verwendet ebenfalls RC4.

Trojaner

Trojaner sind Programme, die sich als gutartige Anwendungen "tarnen". Trojaner sind keine Viren, da sie sich nicht fortpflanzen, können Ihrem Computer jedoch einen ähnlich Schaden zufügen wie Viren.

Überwachte Dateitypen

Die Dateitypen (beispielsweise .DOC, .XLS usw.), die von der Datensicherung innerhalb der Überwachungs-Speicherorte gesichert oder archiviert werden.

Überwachungs-Speicherorte

Die Ordner auf Ihrem Computer, die von der Datensicherung überwacht werden.

Unerwünschte Zugriffspunkte

Ein Zugriffspunkt, den ein Unternehmen für den Betrieb nicht autorisiert. Das Problem dabei ist, dass nicht autorisierte Zugriffspunkte oft nicht den Sicherheitsrichtlinien für WLANs (Wireless LAN, Funk-LAN) entsprechen. Ein nicht autorisierter Zugriffspunkt bietet eine offene, unsichere Schnittstelle in das Unternehmensnetzwerk von außerhalb der physikalisch kontrollierten Einrichtung.

In einem ordnungsgemäß gesicherten WLAN richten nicht autorisierte Zugriffspunkte mehr Schäden an als nicht autorisierte Benutzer. Wenn wirksame Authentifizierungsmechanismen vorhanden sind, müssen nicht autorisierte Benutzer beim Versuch, auf ein WLAN zuzugreifen, nicht unbedingt auch an wertvolle Ressourcen des Unternehmens gelangen. Zu größeren Problemen kommt es jedoch, wenn sich ein Mitarbeiter oder Hacker über den nicht autorisierten Zugriffspunkt anmeldet. Ein nicht autorisierter Zugriffspunkt erlaubt praktisch jedem, der über ein 802.11-kompatibles Gerät verfügt, den Zutritt in das Unternehmensnetzwerk. Dadurch gelangt man schnell sehr nah an geschäftskritische Ressourcen.

URL

Uniform Resource Locator. Hierbei handelt es sich um das Standardformat für Internetadressen.

USB-Drahtlosadapter-Karten

Eine erweiterbare serielle Schnittstelle mit Plug-and-Play-Funktionalität. Diese Schnittstelle bietet eine standardisierte und preisgünstige drahtlose Anschlussmöglichkeit für Peripheriegeräte wie Tastaturen, Mäuse, Joysticks, Drucker, Scanner, Speichergeräte und Videokameras.

Veröffentlichen

Eine gesicherte Datei öffentlich im Internet verfügbar machen.

Verschlüsselung

Ein Vorgang, bei dem Daten von Text in Code umgewandelt werden, wodurch die Informationen verschleiert werden, so dass Personen, die den Code nicht entschlüsseln können, sie nicht lesen können.

Verwaltetes Netzwerk

Ein privates Netzwerk mit zwei Arten von Mitgliedern: verwaltete Mitglieder und unverwaltete Mitglieder. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren McAfee-Schutzstatus einzusehen, unverwaltete Mitglieder tun das nicht.

Vollständige Archivierung

Die Archivierung eines kompletten Datensatzes basierend auf den von Ihnen festgelegten überwachten Dateitypen und Speicherorten.

VPN (Virtual Private Network)

Ein Netzwerk, das entsteht, indem Knoten unter Verwendung von öffentlichen Leitungen neu miteinander verbunden werden. Es gibt zum Beispiel eine Reihe von Systemen, mit denen Sie Netzwerke erstellen können, die das Internet als Medium für den Datentransport verwenden. Diese Systeme setzen Verschlüsselung und andere Sicherheitsmechanismen ein, um sicherzustellen, dass nur autorisierte Benutzer auf das Netzwerk zugreifen und die Daten nicht abgefangen werden können.

Wardriver

Das sind mit Notebooks bewaffnete Eindringlinge, die mit spezieller Software und modifizierter Hardware durch die Gegend streifen, um Datenverkehr von Funk-LANs abzufangen.

Web-Bugs

Kleine Grafikdateien, die sich selbst in Ihre HTML-Seiten einbetten können und es einer nicht autorisierten Quelle erlauben, Cookies auf Ihrem Computer zu platzieren. Diese Cookies können dann Informationen an die nicht autorisierte Quelle übertragen. Web-Bugs sind auch als Web-Beacons, Pixel-Tags, durchsichtige GIFs oder unsichtbare GIFs bekannt.

Weiße Liste

Eine Liste der Websites, denen der Zugriff erlaubt wird, da sie nicht als betrügerische Websites angesehen werden.

WEP (Wired Equivalent Privacy)

Ein Verschlüsselungs- und Authentifizierungsprotokoll aus dem Standard 802.11. Die anfänglichen Versionen basieren auf RC4-Verschlüsselungen und haben beträchtliche Schwächen. Der Sicherheitsansatz von WEP besteht darin, dass per Funk übertragene Daten verschlüsselt werden, damit sie geschützt sind, wenn sie von einem Endpunkt zum anderen übertragen werden. Es hat sich jedoch herausgestellt, dass WEP nicht so sicher ist, wie man ursprünglich angenommen hatte.

Wi-Fi (Wireless Fidelity)

Dieser Begriff wird allgemein für alle Arten von 802.11-kompatiblen Netzwerken verwendet, sei es 802.11b, 802.11a, Dual-Band usw. Der Begriff wird von der Wi-Fi Alliance verwendet.

Wi-Fi Alliance

Eine Organisation, die aus führenden Anbietern von drahtloser Hardware und Software besteht und deren Ziel darin liegt, (1) allen 802.11-basierten Produkten die gegenseitige Kompatibilität zu zertifizieren und (2) den Begriff "Wi-Fi" in allen Märkten für Produkte für 802.11-basierte Funk-LANs als globalen Markennamen zu fördern. Die Organisation dient als Konsortium, Testlabor und Clearinghouse für Anbieter, die die gegenseitige Kompatibilität und das Wachstum dieser Branche voranbringen möchten.

Auch wenn alle Produkte der Standards 802.11a/b/g als Wi-Fi bezeichnet werden, dürfen nur die Produkte, die den Test der Wi-Fi Alliance bestanden haben, das Prädikat "Wi-Fi Certified" (eine eingetragene Marke) tragen. Produkte, die den Test erfolgreich bestanden haben, müssen ein Identifikationssiegel auf ihrer Verpackung haben, auf dem "Wi-Fi Certified" sowie das verwendete Funkfrequenzband stehen. Die Wi-Fi Alliance war früher unter der Bezeichnung Wireless Ethernet Compatibility Alliance (WECA) bekannt, änderte jedoch im Oktober 2002 ihren Namen, um die Marke "Wi-Fi" besser darstellen zu können, deren Aufbau das Ziel der Gruppe ist.

Wi-Fi Certified

Produkte, die von der Wi-Fi Alliance getestet und als Wi-Fi Certified (eine eingetragene Marke) zugelassen wurden, sind als miteinander vollständig kompatibel zertifiziert, auch wenn sie von unterschiedlichen Herstellern stammen. Ein Benutzer eines Produkts mit dem Prädikat "Wi-Fi Certified" kann einen Zugriffspunkt einer beliebigen Marke zusammen mit Clienthardware anderer Marken, die ebenfalls zertifiziert sind, verwenden. Üblicherweise funktionieren Wi-Fi-Produkte mit allen anderen Produkten zusammen, die dieselbe Funkfrequenz verwenden (z. B. 2,4 GHz bei 802.11b oder 11g; 5 GHz bei 802.11a), auch wenn diese nicht das Prädikat "Wi-Fi Certified" haben.

Wiederherstellen

Abrufen einer Kopie einer Datei aus dem Online-Sicherungs-Repository oder einem Archiv.

WLAN (Wireless Local Area Network)

Siehe auch LAN. Ein LAN, das ein drahtloses Medium zum Verbinden verwendet. In WLANs erfolgt die Kommunikation zwischen den Knoten über hochfrequente Funkwellen anstelle von Kabeln.

Wörterbuchangriff

Bei diesen Angriffen wird versucht, ein Kennwort zu ermitteln, indem unzählige Wörter aus einer Liste durchprobiert werden. Dabei geben die Angreifer diese Wörter und alle ihre Kombinationen nicht selbst manuell ein, bis sie das Kennwort von jemandem ermittelt haben, sondern verwenden dafür Tools, die diesen Vorgang automatisieren.

WPA (Wi-Fi Protected Access)

Ein Spezifikationsstandard, der das Niveau von Datenschutz und Zugriffskontrolle bei vorhandenen und zukünftigen Funk-LAN-Systemen stark erhöht. WPA ist vom Standard IEEE 802.11i abgeleitet und damit kompatibel und für die Ausführung auf vorhandener Hardware in Form eines Softwareupgrade entworfen. Bei korrekter Installation bietet es Benutzern von Funk-LANs ein hohes Maß an Sicherheit dafür, dass ihre Daten geschützt bleiben und nur autorisierte Netzwerkbenutzer auf das Netzwerk zugreifen können.

WPA-PSK

Ein spezieller WPA-Modus, der für Privatanwender entworfen wurde, die keine starke Sicherheit wie in Unternehmen üblich benötigen und keinen Zugriff auf Authentifizierungsserver haben. In diesem Modus kann der Privatanwender das Startkennwort manuell eingeben, um WPA im PSK-Modus zu aktivieren, und sollte die Passphrase auf jedem drahtlosen Computer und Zugriffspunkt regelmäßig ändern. Siehe auch WPA2-PSK und TKIP.

WPA2

Siehe auch WPA. WPA2 ist eine Aktualisierung des WPA-Sicherheitsstandards und basiert auf dem 802.11i IEEE-Standard.

WPA2-PSK

Siehe auch WPA-PSK und WPA2. WPA2-PSK ist WPA-PSK ähnlich und basiert auf dem WPA2-Standard. Eine häufig verwendete Funktion von WPA2-PSK ist, dass Geräte häufig mehrere Verschlüsselungsmodi (z. B. AES, TKIP) gleichzeitig unterstützten, während ältere Geräte üblicherweise nur jeweils einen Verschlüsselungsmodus unterstützten (d. h., alle Clients müssten denselben Verschlüsselungsmodus unterstützen).

Wurm

Würmer sind sich selbst replizierende Viren, die sich im Arbeitsspeicher eines Computers befinden und Kopien von sich selbst per E-Mail verbreiten. Würmer replizieren und verbrauchen Systemressourcen, wodurch die Leistung herabgesetzt und Tasks angehalten werden.

Zugriffspunkt

Ein Netzwerkgerät, das 802.11-kompatiblen Clients die Verbindung zu einem LAN (Local Area Network) ermöglicht. Zugriffspunkte erweitern die physikalische Betriebsreichweite für drahtlose Benutzer. Sie werden auch als drahtlose Router bezeichnet.

Info zu McAfee

McAfee, Inc., mit Hauptsitz in Santa Clara, Kalifornien (USA), ist Marktführer im Bereich Intrusion Prevention und Security Risk Management und bietet weltweit präventive und bewährte Lösungen und Services zum Schutz von Systemen und Netzwerken. Dank der unübertroffenen Sicherheitsexpertise von McAfee und seiner Verpflichtung zur Innovation sind private Nutzer, Unternehmen, der öffentliche Sektor und Service Provider in der Lage, Angriffe abzuwehren, Störungen zu vermeiden und ihre Sicherheit kontinuierlich zu verfolgen und zu verbessern.

Copyright

Copyright i 2006 McAfee, Inc. Alle Rechte vorbehalten. Kein Teil dieser Veröffentlichung darf ohne schriftliche Erlaubnis von McAfee, Inc. in irgendeiner Form oder mit irgendwelchen Mitteln vervielfältigt, übertragen, transkribiert, in einem Informationsabrufsystem gespeichert oder in eine andere Sprache übersetzt werden. McAfee und andere hier erwähnten Marken sind eingetragene Marken oder Marken von McAfee, Inc. und/oder Tochtergesellschaften in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit steht unverkennbar für alle McAfee Markenprodukte. Alle anderen hier erwähnten eingetragenen und nicht eingetragenen Marken und unter Copyright stehenden Materialien sind ausschließlich Eigentum ihrer jeweiligen Inhaber.

MARKEN

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (UND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE UND DESIGN, CLEAN-UP, DESIGN (STILISIERTES E), DESIGN (STILISIERTES N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (UND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (UND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M UND DESIGN, MCAFEE, MCAFEE (UND IN KATAKANA), MCAFEE UND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (UND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, QUICKCLEAN,RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (UND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (UND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS.

Index

8

802.11 180
802.11a....180
802.11b 180
802.11g....180
802.1x....181

A

Abrufen des Administratorkennworts ...28
Aktualisieren der Firmware des Routers oder Zugriffspunkts....145
Aktualisieren des drahtlosen Adapters 152
Aktuelle Schlüssel anzeigen 120, 144
Akzeptieren einer Datei von einem anderen Computer....173, 174
An geschützten drahtlosen Netzwerken anmelden 83, 86, 107, 148
Andere Probleme....155
Ändern der Anzeigeeigenschaften eines Geräts 72
Ändern der Berechtigungen eines verwalteten Computers 71
Ändern des Administratorkennworts.....28
Anmelden am verwalteten Netzwerk.....63
Anmelden an einem verwalteten Netzwerk.... 63, 163, 167
Anschluss 181
Anzahl der monatlich geschützten Computer ansehen 136, 137, 138, 140
Anzahl der Schlüsselrotationen einsehen 120, 121, 122, 123, 125, 137
Anzahl der täglichen Verbindungen ansehen.... 136, 138, 140
Anzeigen der Elementdetails....62
Anzeigen der SecurityCenter-Informationen 20
Anzeigen oder Verbergen von Elementen in der Netzwerkzuordnung 62
Anzeigen von Informationen zum installierten Produkt 20
Arbeiten mit der Netzwerkzuordnung...60
archivieren 181
Auf welchen Computern muss diese Software installiert werden? 142
Aufforderung zur Eingabe des WEP-, WPA- oder WPA2-Schlüssels 151
Ausführen häufiger Tasks 37
Auswahl eines anderen Sicherheitsmodus 157
Authentifizierung 181
Automatische Schlüsselrotation aussetzen 107, 122, 124, 150, 151
Automatisches Beheben von Sicherheitsproblemen 19
Automatisches Herunterladen und Installieren von Updates 30
Automatisches Herunterladen von Updates 30, 31
Automatisches Prüfen auf Updates 30
Automatisches Warten Ihres Computers 39

B

Bandbreite 181
Beheben von Sicherheitslücken....73
Beheben von Sicherheitsproblemen 19
Bei Verwendung anderer Programme lautet der Netzwerkname anders....155
Benachrichtigen vor dem Herunterladen von Updates 30, 32
Benachrichtigung bei gesendeter Datei erhalten....174
Bereinigen Ihres Computers 45
Bevorzugte drahtlose Netzwerke entfernen 102, 103
Bevorzugte Netzwerke auflisten... 102, 103
Bibliothek....181
Bilderanalyse 182
Bin ich geschützt?....13
Browser 182
Brute-Force-Angriff....182

C

chiffrierter Text....182
Client 182
Computer im Netzwerk nicht mehr als vertrauenswürdig einstufen 67
Computer zum geschützten drahtlosen Netzwerk hinzufügen85, 91, 95, 148, 151
Computern administrativen Zugriff gewähren 83, 92
Cookie 183
Copyright 200

D

Dateien freigeben 170
Dateien freigeben und senden 169
Dauer der Netzwerkverbindung ansehen 130, 131, 132, 133, 134, 135
Deaktivieren von automatischen Updates 30, 32, 34
Defragmentieren von Dateien und Ordnern 41
Dem Netzwerk beitreten.....164
Denial of Service, DoS.....183
Derzeit geschützte Computer ansehen 101, 137, 138, 140
DNS.....184
DNS-Server 184
Domäne.....184
Download schlägt auf sicherem Netzwerk fehl.....144
Drahtlose Netzwerke schützen.....81
Drahtlose Netzwerke überwachen.....129
Drahtlose Netzwerkverbindungen überwachen.130, 131, 132, 133, 134, 135
Drahtlose Router oder Zugriffspunkte entfernen 107, 109, 144, 148
Drahtlose Router oder Zugriffspunkte konfigurieren.....156
Drahtlosen Netzwerken verwalten.....99
Drahtloser Adapter.....184
Drucker freigeben.....175

E

EasyNetwork einrichten.....161
EasyNetwork starten 162
Echtzeit-Scans 184
Eine Datei an einen anderen Computer senden.....173
Einladen eines Computers, sich am verwalteten Netzwerk anzumelden 65
E-Mail 184
E-Mail-Client 184
Entfernen nicht verwendeter Dateien und Ordner.....40
Ereignis.....185
Erläuterung der Network Manager-Symbole.....57
Erläuterungen zu den Funktionen von Shredder 50
Erläuterungen zu den QuickClean-Funktionen.....44
Erläuterungen zu den Schutzkategorien und -typen 14
Erläuterungen zu den SecurityCenter-Symbolen 11
Erläuterungen zu E-Mail- und IM-Schutz 17
Erläuterungen zum Parental Controls-Schutz 18
Erläuterungen zum Schutz von Computer und Dateien.....15
Erläuterungen zum Schutz von Internet und Netzwerk.....16
Erläuterungen zum Schutzstatus.....13
Ersetzen von Computern.....157
Erstellen eines Administratorkontos 25, 26
Erstellen eines verwalteten Netzwerks ..59
ESS (Extended Service Set) 186
Externe Festplatte.....186

F

Fehler bei der Schlüsselrotation.....146
Fehler durch doppelte Administratoren 145
Firewall.....186
Freigabe einer Datei.....170
Freigabe einer Datei aufheben.....171
Freigabe eines Druckers aufheben 176
Freigeben 187
Freigegebene Datei kopieren 171
freigegebenes Geheimnis 187
Funktionen 8, 44, 50, 56, 76, 160

G

Geschützte drahtlose Netzwerke einrichten 82
Geschützte drahtlose Netzwerke erstellen 84, 109, 147
Geschützte drahtlose Netzwerke überwachen..... 136, 137, 138, 140
Geschützte drahtlose Netzwerke umbenennen..... 104, 107
Geschützte drahtlose Netzwerke verlassen..... 110, 111, 112, 148
Geschützte drahtlose Netzwerkereignisse ansehen 136, 137, 138, 139, 140
Gewähren von Zugriff für einen unbekannten Computer.....148

H

Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie96, 97, 125, 144
Hinzufügen von Computern über Wechselgeräte 95, 98, 144
Hotspot 187

I

Info zu McAfee.....199

Informationen für drahtlose Geräte ändern 107, 117, 146
Inhaltsklassifikationsgruppen 187
Installieren der McAfee-Sicherheits-Software auf Remote-Computern.....74
Installieren eines verfügbaren Netzwerkdruckers 177
Installieren von Wireless Network Security 142
integriertes Gateway.....187
Internet.....187
Intranet.....187
IP-Adresse 188
IP-Spoofing 188
isolieren.....188

K

Kennwort.....188
Kennwort-Tresor 188
Knoten.....188
Kompatibler drahtloser Adapter wird nicht erkannt 143
Komprimierung 189
Konfigurieren der Update-Optionen 29
Konfigurieren des Schutzstatus.....24
Konfigurieren ignorierter Probleme.....24
Konfigurieren von Alarmoptionen 35
Konfigurieren von Benutzeroptionen ...25, 27
Konfigurieren von Informationswarnungen 36
Konfigurieren von SecurityCenter-Optionen 23
Konfigurieren von Sicherheitseinstellungen 114, 157
Konfigurieren von Warnoptionen 35
Kopfzeile.....189

L

LAN (Local Area Network) 189

M

MAC (Media Access Control oder Message Authenticator Code) 189
MAC-Adresse (Media Access Control Address) 189
Manuelles Beheben von Sicherheitsproblemen 19
Manuelles Prüfen auf Updates 32, 34
Manuelles Warten Ihres Computers 40
MAPI-Konto 189
McAfee EasyNetwork 159
McAfee Network Manager 55
McAfee QuickClean.....43
McAfee SecurityCenter 7
McAfee Shredder.....49
McAfee Wireless Network Security 75
McAfee Wireless Protection.....5
Mehrere drahtlose Adapter 144
Mit freigegebenen Druckern arbeiten .176
MSN-Konto.....189

N

Netzwerk.....189
Netzwerk scheint ungeschützt 147
Netzwerk umbenennen 61, 166
Netzwerk-Laufwerk.....190
Netzwerkschlüssel löschen.....128
Netzwerkschlüssel manuell rotieren ..125, 137, 150
Netzwerkschlüssel verwalten 119, 137
Netzwerk-Sicherheitseinstellungen konfigurieren.....116
Netzwerk-Sicherheitseinstellungen reparieren 107, 116, 118, 146, 152
Netzwerksicherheitsmodus ansehen..101, 116, 132, 157
Netzwerkverbindungsgeschwindigkeit ansehen 130, 131, 132, 133, 134, 135
Netzwerkzugriffsrechte aufheben ... 83, 92, 107, 110, 111, 112
Netzwerkzuordnung 190
Netzwerkzuordnung aktualisieren 61
NIC (Network Interface Card, Netzwerkkarte).....190
Nicht unterstützter Router oder Zugriffspunkt.....145

O

Öffnen des Konfigurationsbereichs für 15, 16, 17, 18
Öffnen des SecurityCenter-Konfigurationsbereichs 20
Öffnen von SecurityCenter und Verwenden der zusätzlichen Funktionen.....11
Online-Sicherheitsbericht ansehen 130, 131, 132, 133, 134, 135, 143
Online-Sicherungs-Repository.....190

P

Parental controls 190
PCI-Drahtlosadapter-Karte 190
Phishing 190
POP3-Konto 190
Popups 190

Potentiell unerwünschtes Programm ..191
PPPoE ..191
Problembehandlung ..141
Protokoll ..191
Proxy ..191
Proxy-Server ..191
Prüfen des Status Ihrer Updates ..12
Prüfen Ihres Schutzstatus ..11
Pufferüberlauf ..191

R

RADIUS (Remote Access Dial-In User Service) ..191
Referenz ..179
Reiner Text ..191
Remote-Verwaltung des Netzwerks ..69
Reparieren des Routers oder Zugriffspunkts nicht möglich ..146
Roaming ..191
Router ..192

S

Säubern Ihres Computers ..47
Schlüssel ..192
Schlüssel als Sternchen darstellen 126, 127
Schlüssel automatisch rotieren ..107, 121, 122, 123, 124, 125, 137, 146, 150
Schlüssel in Klartext anzeigen ..126, 127
Schlüsselrotation fortsetzen 121, 122, 125, 150
Schlüsselrotationshäufigkeit anpassen ..121, 122, 125
Schnellarchivierung ..192
Schutz anderer drahtloser Geräte ..85, 93
Schützen oder Konfigurieren des Netzwerks ..144
Schwaches Signal ..153
Schwarze Liste ..192
Senden von Dateien an andere Computer ..173
Server ..192
Sicherheit für drahtloses Netzwerk verwalten ..113
Sicherheitslücken schließen ..73
Sicherheitsmodi konfigurieren ..114
sichern ..192
Signalstärke des Netzwerks ansehen ..101, 134, 153
Skript ..192
SMTP-Server ..192
Software funktioniert nach Aktualisierung des Betriebssystems nicht ..158
Speicherort für die oberflächliche Überwachung ..193
Speicherort für umfassende Überwachung ..193
SSID (Service Set Identifier) ..193
SSL (Secure Sockets Layer) ..193
Standard-E-Mail-Konto ..193
Starten von EasyNetwork ..162
Stichwort ..193
Stoppen der Überwachung des Schutzstatus eines Computers ..71
Suchen nach einer freigegebenen Datei ..171
Synchronisieren ..193
SystemGuard ..194

T

TKIP (Temporal Key Integrity Protocol) ..194
Trojaner ..194

U

Über Wireless Network Security-Symbole ..100, 131
Über Zugriffstypen ..83, 92
Übergehen zur Verwendung von McAfee-Benutzerkonten ..25
Überwachen des Schutzstatus eines Computers ..70
Überwachen des Status und der Berechtigungen ..70
Überwachte Dateitypen ..194
Überwachungs-Speicherorte ..194
Unerwünschte Zugriffspunkte ..194
URL ..194
USB-Drahtlosadapter-Karten ..195

V

Verbinden von Computern mit Ihrem Netzwerk ..147
Verbindung unterbrochen ..150
Verbindung zu geschützten drahtlosen Netzwerken ..91, 107, 108
Verbindung zu Netzwerken mit deaktivierter SSID-Übertragung ..93
Verbindung zum drahtlosen Netzwerk nicht möglich ..151
Verbindung zum geschützten drahtlosen Netzwerk aufheben ..107, 110, 111, 112
Verbindung zum Internet kann nicht hergestellt werden ..150
Verbindung zum Internet und Netzwerk aufbauen ..149
Verbindungsbenachrichtigung anzeigen ..108

Verbindungsstatus ansehen 130, 131, 132, 133, 134, 135
Verbindungsverlust bei Geräten.....151
Vernichten unerwünschter Dateien mit Shredder 51
Vernichten von Dateien, Ordnern und Datenträgern 52
Veröffentlichen 195
Verschieben von Updates auf einen späteren Zeitpunkt.....31, 33
Verschlüsselung.....195
Verwalten drahtloser Netzwerke 100
Verwalten eines Geräts.....72
Verwalten Ihres Netzwerks 42
Verwaltetes Netzwerk.....195
Verwaltetes Netzwerk verlassen 167
Verwenden des Menüs.....21
Verwenden von QuickClean 47
Verwenden von SecurityCenter.....9
Verwenden von Shredder 52
Vollständige Archivierung.....195
VPN (Virtual Private Network) 195

W

Wardriver 195
Warneinstellungen konfigurieren 105
Warten auf Autorisierung.....148
Web-Bugs 195
Weiße Liste.....195
Weitere Informationen zu Viren.....42
WEP (Wired Equivalent Privacy) 196
Wiederherstellen 196
Wi-Fi (Wireless Fidelity) 196
Wi-Fi Alliance.....196
Wi-Fi Certified 196
Windows unterstützt keine drahtlose Verbindung.....154
Windows zeigt keine Verbindung an....154
Wireless Network Security deaktivieren 79
Wireless Network Security starten .78, 151
WLAN (Wireless Local Area Network) ..196
Wörterbuchangriff.....197
WPA (Wi-Fi Protected Access) 197
WPA2 197
WPA2-PSK 197
WPA-PSK 197
Wurm.....197

Z

Zugreifen auf die Netzwerkzuordnung ..60
Zugriff auf das Netzwerk gewähren.....165
Zugriffspunkt 197
Zuletzt aufgetretene Ereignisse anzeigen 38
Zurücksetzen Ihres Computers auf die vorherigen Einstellungen 41